

**UNIVERSITY OF GAZIANTEP
GRADUATE SCHOOL OF
NATURAL & APPLIED SCIENCES**

**DESIGN AND IMPLEMENTATION OF A NETWORK FOR
HOSPITAL INFORMATION SYSTEM**



**M.Sc. THESIS
IN
ELECTRICAL AND ELECTRONICS ENGINEERING**

BY

ABDULQADER RASOOL FEQI MOHAMMED

MAY 2016

**Design and Implementation of a Network for Hospital
Information System**

M.Sc. Thesis

in

Electrical and Electronics Engineering

University of Gaziantep

Supervisor

Prof. Dr. Ergun ERÇELEBİ

By

Abdulqader Rasool Feqi MOHAMMED

May 2016



© 2016 [Abdulqader Rasool Feqi MOHAMMED]

REPUBLIC OF TURKEY
UNIVERSITY OF GAZİANTEP
GRADUATE SCHOOL OF NATURAL & APPLIED SCIENCES
ELECTRICAL AND ELECTRONIC ENGINEERING DEPARTMENT

Name of the Thesis: Design and implementation of a network for hospital information System

Name of the student: Abdülqader Rasool Feqf MOHAMMED

Exam date. 23 May, 2016

Approval of the Graduate School of Natural and Applied Sciences

Prof. Dr. Metin BEDİR

Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.


Prof. Dr. Ergun ERÇELEBİ

Head of Department

This is to certify that we have read this thesis and that in our opinion, it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.


Prof. Dr. Ergun ERÇELEBİ

Supervisor


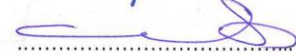

Examining Committee Members:

Prof. Dr. Ergun ERÇELEBİ

Assoc. Prof. Dr. Mustafa YILMAZ

Assoc. Prof. Dr. Fatih HASÖGLU

Signature

That information contained and document that was resaved in agreement for the rules of academic and ethical conduct. I also knowing that, as needed by these rules, I have fully cited and referenced all the subjects and outcomes that are not a native to my research.

Abdulqader Rasool Feqi MOHAMMED

ABSTRACT

DESIGN AND IMPLEMENTATION OF A NETWORK FOR HOSPITAL INFORMATION SYSTEM

MOHAMMED, Abdulqader Rasool Feqi
M.Sc. in Electrical-Electronics Engineering
Supervisor: Prof. Dr. Ergun ERÇELEBİ
May 2016
Pages 95

A special challenge is the coordination of the hospitals buildings with using the most common requirements in health care facilities, building control system and electric power distribution, hospital information system (HIS) , using computer network to implementation this hospital information system and using protection against intrusion. It is important to ensure that data in transit should not be accessed, modified or tampered by unauthorized persons. Unauthorized access to data may cause heavy damage.

Hospital Information System (HIS) is considered as an important factor in health care sector for managing the administrative, financial and clinical aspects of a hospital. The purpose of this project is to research on new network design that has a security techniques in order to enhance the current network security structure of save a hospital information system (HIS). This is very important because, it will avoid the system from suffering any attack. Security architecture was optimized but there are need to keep researching on best means to protect the network from future attacks. In this final project research, security techniques were uncovered to produce best network security results by using internet security protocols and adding a firewall, when implemented in an integrated frame work.

Key words: Hospital information system, HIS, Internet protocol, IP.

ÖZET

HASTANE BİLGİ SİSTEMİ İÇİN TASARIM VE BİR AĞ UYGULANMASI

MOHAMMED, Abdulqader Rasool Feqi

Yüksek Lisans Tezi, Elektrik-Elektronik Mühendisliği

Tez yöneticisi: Prof. Dr. Ergun ERÇELEBİ

Mayıs 2016

95 sayfa

Çalışmanın özel amacı hastane yapımı sırasında kullanılan materyallerin kontrolü ,hastanenin yapımını kontrol eden sistemin elektrik dağılımı , internet ağını kullanarak hastane bilgi sistemini ihlallerden korumak , yönetmek ve bu bilgileri yetkili olmayan kişilerden korumak ve sistem bilgisinde izinsiz düzenleme yapmamalarını ve zarar vermemelerini sağlamak içindir.

Sağlık hizmetleri genel sektörü, hastanenin genel yönetimi, finansal yönetimi ve klinik yönetiminde hastane bilgi sistemi önemli bir rol oynar. Hastane bilgi sisteminin birikiminin ağ akımını koruması ve güvenliği sağlamak için güvenlik tekniklerine sahip olan yeni bir ağ dizaynları üzerinde araştırma yapmayı amaçlamaktır. Bu çok önemlidir çünkü bu sistemi saldırılardan, problemlerden uzak tutmayı sağlayacak ve bazı mimari yapı optimize edilmiş olmasına rağmen gelecekteki saldırılardan korumak için bazı incelemelerin takibi için gereklidir. Bu son araştırma projemde bir yapının birleştirilmesinde , internet güvenlik protokolünü ve güvenlik duvarını ekleyerek daha başarılı güvenlik ağını oluşturma amaçlıdır.

Anahtar Kelimeler: Hastane bilgi sistemi, HIS, Internet protokolü, IP.



Dedicated to

My Country and my all family

ACKNOWLEDGEMENT

First and foremost I would like to acknowledge Almighty God who granted me wisdom, health and strength to overcome life's difficulties and actualizing my set targets and academic achievement.

I want to thanks my supervisor, Prof. Dr. Ergun ERÇELEBİ, for continuous support my M.Sc. research, for his ongoing advice, encouragements, the great moral motivation, patience, brotherly treatment and insight throughout the writing of this research work. My gratitude is due to the staff for the assistant and support through the years of my study and research. I want to show gratitude with my love to my family for support and love through the duration of my M. Sc. life. They have given me an endless enthusiasm.

TABLE OF CONTENT

	page
ABSTRACT	v
ÖZET	vi
ACKNOWLEDGEMENT	viii
TABLE OF CONTENT	ix
LIST OF FIGURES	xii
LIST OF SYMBOLS/ABBREVIATIONS	xv
CHAPTER 1	1
INTRODUCTION	1
1.1 Objective of the thesis.....	2
1.2 System needs	2
1.3 Network security	3
1.4 Network security attributes	3
1.5 Threats of the Networks	4
1.6 Reducing of Physical Threats.....	5
1.7 The Attacks of the network	6
1.8 Arrangement of the thesis.....	9
CHAPTER 2	11
BACGROUNED	11
2.1 Computer Networks	11
2.2 Network Classification.....	11
2.2.1 Network Topologies	14
2.2.2 Type of cables that used in networks	17
2.2.3 Medium access control	19
2.2.4 Network Protocols	20
2.3 Electrical Networks	21
2.3.1 Electrical circuits types.....	21
2.3.2 Planning and Reduction the Cost for the electrical networks	23

2.3.3 Basic Consideration on Power Distribution	24
2.3.4 Electrical Power Distribution Systems Drafting in electrical network	24
2.3.5 Supply and operating Voltages in Distribution Grids	25
2.3.6 Type of Power Supply	26
2.3.7 Network Configurations	26
2.4 HIS.....	28
2.4.1 Patient care	29
2.4.2 Administration	30
2.4.3 Account system	30
2.5 Some monitoring programs.....	31
CHAPTER 3	32
SYSTEM ARCHITECTURE	32
3.1 Overview.....	33
3.1.1 User	33
3.1.2 A Client.....	33
3.1.3 Switch	34
3.1.4 Cost analysis for different brands of Switches.....	35
3.1.5 Router.....	37
3.1.6 Firewall.....	40
3.1.7 Firewall types.....	41
3.1.8 Firewall techniques and details.....	41
CHAPTER 4.....	43
ELECTRICAL REQUIREMENTS FOR A HOSPITAL	43
4.1 Review of the Plan.....	43
4.2 Electrical system	44
4.3 Emergency power system	44
4.4 Conduit and wiring	45
4.5 Communications and signal systems.....	46
4.6 Non-patient area branches needed	46
4.7 Patient area branches needed	46
CHAPTER 5.....	48

ENFORCING NETWORK SECURITY BY CONFIGURATIONS DESIGNED MODEL.....	48
5.1 Introduction	48
5.2 Configuration of external sources	48
5.3 Configuration of switch, S 1.....	49
5.4 Configuration of switch, 2S.....	55
5.5 Configuration of switch, 3S.....	59
5.6 Configuration of switch, 4S.....	67
5.7 Configuration of Router, R 1.....	76
5.8 Configure PC to local area network.....	86
5.9 Configure Firewall.....	88
CHAPTER 6.....	90
CONCLUSION AND SUGGESTION FOR FUTURE WORK	90
6.1 CONCLUSION	90
6.2 Suggestion for future works	90
REFERENCES	92

LIST OF FIGURES

	page
Figure 1 (PAN).....	12
Figure 2 (LAN).....	12
Figure 3 Metropolitan Area Network	13
Figure 4 Wide Area Network	13
Figure 5 Line Topology.....	14
Figure 6 Bus topology	14
Figure 7 Ring topology	15
Figure 8 Tree topology	16
Figure 9 Star topology.....	16
Figure 10 Mesh topology	17
Figure 11 fully connected topology	17
Figure 12 Twisted pair cable	18
Figure 13 Coaxial cable.....	18
Figure 14 Optical fiber cable.....	19
Figure 15 Ethernet cable	19

Figure 16 Series Circuit.....	22
Figure 17 Parallel Circuit	22
Figure 18 Series Parallel Circuit	23
Figure 19 Voltage levels between the power station and the consumer	25
Figure 20 Type of power supply	26
Figure 21 Radial network	27
Figure 22 Mesh network	28
Figure 23 Hospital information system.....	29
Figure 24 patient care	29
Figure 25 account system.....	30
Figure 26 system overview	32
Figure 27 type of clients	34
Figure 28 Switches	35
Figure 29 Routers	38
Figure 30 Firewall	40
Figure 31 Pocket filter.....	41
Figure 32 Application gateway.....	41
Figure 33 Circuit level gateway.....	42
Figure 34 Bastion host.....	42
Figure 35 designed mode	49

Figure 36 VLAN 4, 5 on SWITCH, 3	62
Figure 37 VLAN 1, 2, 3, 4 on SWITCH, 4	71
Figure 38 Config.the PC to (LAN) step 1	87
Figure 39 Config.the PC to (LAN) step 2	87
Figure 40 Config.the PC to (LAN) step 3	88
Figure 41 firewall configuration	89



LIST OF SYMBOLS/ABBREVIATIONS

AC	Alternative Current
AES	Advanced Encryption Standard
ATM	Asynchronous Transfer Model
ATS	Automatic Transfer Switch
BGP	Border Gateway Protocol
CB	Circuit breaker
CCU	Coronary care unit
CDDI	Copper Distributed Data Interface
CRC	Cycle Reducing Check
DC	Direct Current
DES	Digital Equipment Corporation
DMZ	Demilitarized Zone
DNS	Data Network Station
DSL	Digital Signal Line
EIGRP	Enhanced Internet Gateway Routing Protocol
ESPS	Emergency Standby Power Supply
FDDI	Fiber-Distributed Data Interface
FWTK	Firewall Toolkit
HIS	Hospital Information System

HZ	Hertz
I	Current
ICMP	Internet control message protocol
ICU	Intensive care unit
IDRP	ICMP Router Discovery Protocol
IRDP	Internet Router Discovery Protocol
IEEE	Institute of Electrical and Electronic Engineers
IGRP	Internet Gateway Routing Protocol
IHL	IP Header Length
IP	Internet Protocol
IPS	Intrusion prevention system
ISP	Internet Service Provider
IPX	Internet Packet Exchange
KV	Kilo volt
KVA	Kilo Volt Ampere
LSA	link State Advertisement
LV	Low Voltage
MAC	Media access control
MD	Message Digits
MRI	Magnetic Resonance Imaging
MV	Medium Voltage
MW	Mega Watt
NAS	Network Access Server
NICU	Neonatal Intensive Care Unit

NGFW	Next Generation Firewall
NPS	Normal Power Supply
OSHPD	Office of Statewide Health Planning and Development
OSI	Open System Interconnection
OSPF	Open Short Path first
PC	Personal Client
R	Resistance in ohm
RIP	Routing Information Protocol
SMDS	Switch Multimegabit Data Service
SHA	Secure Hash Algorithm
SPF	Short Path first
SPS	Safety Power Supply
SS	Secure Socket layer
SSH	Short for Secure Shell
TCP	Transmission Control Protocol
TIP	Totally Integrated Power
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
V	Volt
VA	Volt Ampere
VPN	Virtual private network
WAF	Web Application Firewall
WEP	Wired Equivalent Privacy
Z	Impedance

CHAPTER 1

INTRODUCTION

In today's global, it is no way to do anything if you are not using the computer to achieve one of the missions or works. The PC becomes a section of daily life, society, especially in the section of daily lives, the computers are used to:

- 1- Archiving and recovering the records in hospitals.
- 2- Purchasing and conducting business transactions online.
- 3- Archiving and recovering the criminal records by the law men.
- 4- Online learning.
- 5- Archiving and recovering of academic records in schools.

In management of these types of recording we need to use the computers, it is very important to saving that data in transferring by preventing the persons that want to accessing, modifying or tampering that data. A computer that using Internet to connection through a (LAN) is more susceptible to attacks like data theft or data processors in comparison with separate computer with an allocated Internet connection such as a (DSL). The cause of this is that, on a LAN some persons can access to your PC or find your data without physical accessing to your PC but if you have some good security actions you can prevent such attempt. With a separate computer, if someone want to access your computer he must physically access to the computer to access data that stored on it. However, if the primary security conditions for every computer is not provided, it is still possible to take your data from the computer far away by using Internet. This brings into incident the subject of network security. That is, securing network devices and the users of the networks access. This thesis will investigate to find on new network security methods to promote this current

network Security structure of save a hospital information system (HIS). This importance must be used to avoid the system from suffering any attack.

1.1 Objective of the thesis

The basic goal in this is to build and design a network that has a good security by using internet security protocols and adding a firewall to implementation a hospital information system and to connect with the ministry of health.

The sub-goals were identified at an early stage of the work:

- 1- Determination the needed devices of a network.
- 2- Researching with the different currently available systems and improving them.
- 3- Designing a system that based on available devices of the state devices and researching for other solutions.
- 4- Analyze the system and specify future improvements.

1.2 System needs

System requirements were determination through from the design stage of the thesis. All networks have the same needs:

- 1- High speed
- 2- Minimum cost
- 3- Easy management
- 4- Ease of use
- 5- Flexibility
- 6- Scalability

Using any system need users and every person must have a profile that contains his information. The system at least used with two types of clients.

The first user is only need to have personal computer in the hospital with:

- 1- The user name and password of the part of the hospital where he working.
- 2- The first user needs to submit IP of the client program.

- To login any system it needs the followings:
 - 1- The user must identified by unique password and user name.
 - 2- Unsuccessful login should be recorded for security purposes.
 - 3- After two times or more unsuccessful login in to the system this user may be blocked for a few minutes.

1.3 Network security

To insure network security we must follow the followings:

- 1- The user should be able to documentation the system before reviling his user name and password.
- 2- For any non-advanced user it must not be possible to change firewall roles.
- 3- Protection from MAC address and IP spoofing must be provided.
- 4- Wire equivalent privacy (WEP) should be used.
- 5- The system should check MAC address (possibility at access point).
- 6- The password must be hashed and never be stored as clear text when provided and stored from the database.
- 7- All unused ports must be closed and all unnecessary accounts may be removed.

1.4 Network security attributes

The security of the networks become more important today's ,the face challenges of the experts of the network security is to deny any persons that want to accessing, stealing or tampering with the data of networks. The security of the network is a way of documenting, encrypting and partitioning directed at protecting network resources from some persons. This way takes into consideration the company's policy, that means who has access to what resources, and who has not access to some resources.

The following are network security properties:

- **Authentication**

To reach a network, we need username and password to approval for using the network. This is authentication [1].

- **Confidentiality**

With transference data through the network, it should be mysterious for those who are not wanted to see this data. To doing this, the data has been hashed symmetrically or asymmetrically. Symmetrical hashing uses mutual sacred key to encrypt and decrypt information [3].

- **Integrity**

During information crossing in the network, the information should be devoid of any exploited by intruders. Data integrity can be conducted by hashing the information sent by using (message digest 5) MD5 or (secure hash algorithm) SHA-1 or SHA- 2. When a hashed message arrive, a hash of the information is calculated and examined against hash that sent by the main computer. If the two hashes have conformity, information integrity has been maintained if not information is rejected for reason of modulation in transit. With hashing impose on information, it is so hard to modify information in crossing without detection. SHA- 2 is the most guaranteed and recommended because it is so difficult to bring two messages that hash to same hash value [4].

- **Availability**

All networks organizations and services must be available at all times to allow the persons at any time they needed it. The meaning of all times lead us to thinking about all of the 24 hours of every day and thinking about all 7 days of every weeks that meaning the availability of all times ; if not, these will leads to enormous loss of production of us [2].

1.5 Threats of the Networks

The threats of all networks are expert people who are ready to investment the weakness of a network security to hurt or damaging the network. They can achieve this by

sending a various assault tools found in the market such as Netcat or self written scripts. These assaulters have names of their various depending on the needing of them, as shown in the following list:

- 1- A hacker – today's, is a people who tries to get unwanted access to network information's with bad intentions. But with that, in the first days a hacker was known to be a very good programmer or a very good coder.
- 2- Blackhat or Cracker – This is a people who tries to gain unwanted access to network resources for bad faith to damage the network.
- 3- Spammer or the individual people, this is a person who is sending a bulk of messages without being required or emails of that content a virus in an supplement aims to harm the computer or to take the information from your computer and forwarding the information's by email to the spammer.
- 4- Phishers – This is person who by using emails or other means scams individually to stilling your data such as your user name, the number of your credit card or your password. They usually camouflage as trusted persons [5].

1.6 Reducing of Physical Threats

The reducing of physical threats in network implementation is very important such that if ignored, they impose a weakness to the network security. Below there are some of physical threats that must be taken in the security of network:

- 1- The threats of hardware can be reduced by saving the devices endpoints in closed rooms to increase security where only some persons can inter this room and can access and by using security monitoring cameras.
- 2- The threats of environmental can be reduced by using fans or heaters or by using new systems in all rooms and using sensors alarms to knowing high or low temperatures such as low or high temperatures can be avoided.
- 3- We can keep the computer running and saving the devices from electrical shutdown by using UPS when power is shutdown. And using standby generators to provide electrical power if a problem happened in the main source this will require a proper shutdown of computer without damages the hard drive.

- 4- We need to reduce maintenance threat by using electrostatic discharge wrist and connecting earthen in maintenance procedure, labeling sensitive cables and stock plenty of spare parts [5].

1.7 The Attacks of the network

There are 4 types of network attacks namely:

- 1- The attack of reconnaissance
- 2- The attack of the access
- 3- The attack of Denial of service
- 4- The attack of Malicious code

- **The attack of reconnaissance**

In this kind of attack or data collection process, various tools uses by the attacker to get the data from network information and its weaknesses. After data collection both username and password, the attacker can attack and if the attacker successful, destruction on the network information is established with possible stealing of information.

- **The attack of the access**

In this type, the attacker person using some things like hacks tools and texts to get access to your computer, or the devices like server, router or data that he is not allowed to access. He can do it by cracking your user name and your password. The attack of the access has various forms as follows:

- 1- The attack of password

This type of attack can be made by using (packet sniffers). In the case that the user name and password is get in simple text for like CISCO, the unwanted person will learn your user name and your password which he could use to get unwanted access to the information of the network and cause damage. Instead of that, the person can use things to get access by using brute-force attack tools like Lophtrcracker or Cain.

These type of person try many times to login and he try to using different words from his self or some words and some numbers. For example SAMAengi1977 is a good way to mitigate brute-force attack because it is more than 8 characters and has capital and small words and numbers.

2- The exploitation of trust

The outside device of the firewall which reliable by a device behind the firewall is breached. When this outside device is breached, the person who unwanted uses the confidence coupling to release attacks on the inside device. To avoid confidence exploitation, making a private VLANs.

3- The redirection of port

In this type of confidence exploitation that is breached device, if the one side of the firewall is used to redirect traffic from an outer device on the Internet to an internal device behind the firewall. This would not have been possible for an outside device to transfer directly with the device behind the firewall if the DMZ device was not breached. When a DMZ host is breached, Netcat is a good software example that an unwanted person can install to redirect traffic to an internal device. However, to deny the port redirection, device based IPS (intrusion prevention system) must be install on a device and configure to deny and log intervention.

4- The attack of man-in-the -middle

In the attack of the man-in-the middle, the person who is in the unwanted place himself between connection devices, for example routers. With a packet sniffer, the unwanted person can have access to lot of data like username, password and content of moved data, if moved data is not encrypted. The attack of man- in-the middle can be greatly prevent by using secure shell for administration network devices like switches and routers, encrypting all wireless traffic and VPN for WAN connections [3].

- **The attack of denial of service (DOS)**

The attack of DOS is a type that invincible the resources of targeted hosts in networks, a router is an example, such that, the router cannot submit its need services. The attack of DOS has various forms as follows:

1- Ping Of Death

This type of the attack DOS amends the IP section of a ping packet header that is between 64-84 bytes to a value of 65535 bytes. This null shows that the IP packet has more information than it actually content. Any device that receives such a packet will in the end damaged. But however, new and modern devices are flexible to this model of attack.

2- Sny flood

In transmission control protocol connection, there are three way handshakes to implementation any connection. An attacking device sends multiple transmission control protocol Sny request, target device for example a router response with Sny Ack response but the attacking device never response with the final acknowledgment to end the three way handshakes. This intentional work by the attacker device causes the router device to run out of resources to serve forensic person.

3- Bomb of email

It is a type of attack where sending big number and big quantity of emails to a receiver with a bad purpose to exhaust his mailbox ability or crush his mail server ability where the mail boxes are added.

4- The distributed attack of denial of service (DDOS)

The distributed attack of denial of service is a more advanced type of denial of service attack. The main purpose is to gratification connection links and target devices with bad information. This will cause links or target devices to drop bad information or request due to want of resources. In DDOS you have the following characters:

a: Computer ,client or a person who begin attack.

b: Handler danger computer that running and works as an attacker programs. A handler can control many dealership (zombies).

c: Dealership - danger device administration attacker programs and is administration for generating big quantity of traffic directed target device. It is very important to know that, in some recent years, 'Botnet' refers to a jargon used to describe a collects of bad software used to release the distributed attack of denial of service attacks [3, 6].

- **The attack of malicious code**

This type of attack on a device caused by a virus, worm or Trojan horse the worm does not need man meddling to spread. From transmission to infected device to a new device. When a worm attacks a device, it copies itself into the device memory and then release attack to another weak device. Worms can act on the device to slow network response because they take network bandwidth. The application that necessary to operating system updates, splatter and device based IPS to reduced worms. A virus unlike a worm, take itself to a file. Virus need man help to spread from one device to another. Its payload may include stopping the computer or damaging the files. To deny this case we can use the method that it include used up to date antivirus or Internet security program.

1.8 Arrangement of the thesis

My thesis is organized into 6 chapters:

Chapter 1 gives introduction of the computer networks, Objective of the thesis, System needs, Network security and Network security attributes Network Threats, Mitigating of Physical Threats Network Attacks and the organization of this project.

Chapter 2 gives background of the computer networks, networks classification, network Topologies, transmission media that used in networks, network medium access control, network protocols , explain electrical networks and hospital information system (HIS) and some monitoring programs.

Chapter 3 gives the network system architecture, system overview and the elements that used in the system.

Chapter 4 gives the electrical requirements for a hospital.

Chapter 5 gives the enforcing network security by configurations designed model, configuration of SWITCH, S1, configuration of SWITCH, S2, configuration of SWITCH S3, configuration of SWITCH, S4, configuration of ROUTER,R1, configuration of PC to local area network and configuration of firewall.

Chapter 6 gives the conclusion and suggestion for future works.



CHAPTER 2

BACKGROUND

2.1 Computer Networks

All networks contain more than one computer. The devices in a network may be connected by 1- cables. 2- Telephone lines. 3- Radio waves. 4-Satellites. 5- IrDA. (Infrared Data Association). 6- More.

2.2 Network Classification

The classification of the networks done by a group of the network. Networks that have little meters range are classified as (PAN). Networks that have some hundred meters range are classified as (LAN). At gathering many (LAN) connected with other, under of some kilometers, the network is named as a (MAN). And if a network ranged in more than some kilometers named as (WAN).

- **(PAN)**

The personal area network are considered to be a personal devices interconnected within a few meters. The contact between the PC and connecting them to above level networks is an example of using of a personal area network, such as Internet [7]. (PAN) may be linked with device like USB and Fire wire. (Wireless PANs) are founded through technologies like IrDA and Bluetooth.

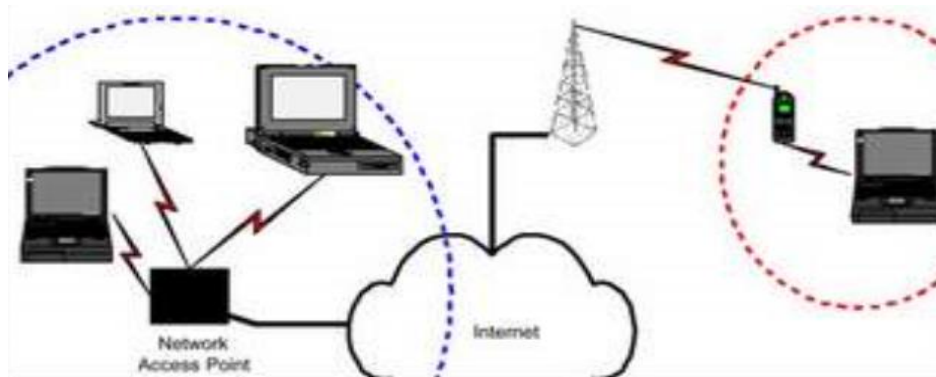


Figure 1 (PAN)

- **Local Area Network (LAN)**

The generally accepted maximum size for a (LAN) is each devices interconnected within an area of 1000m² [2]. The properties which describe a local area network are typically High bandwidth and low latency [9, 10].

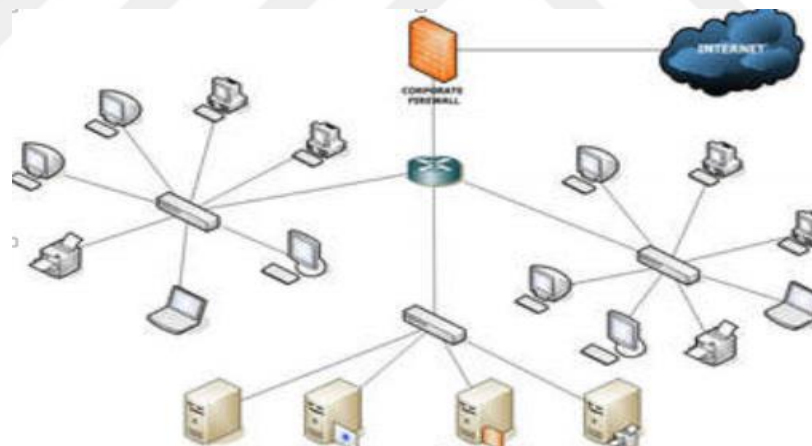


Figure 2 (LAN)

- **(MAN) metropolitan area network**

A large computer networks usually spanning a campus or a city are named as (MANs) or metropolitan area networks. Examples of using (MANs) [7, 9].

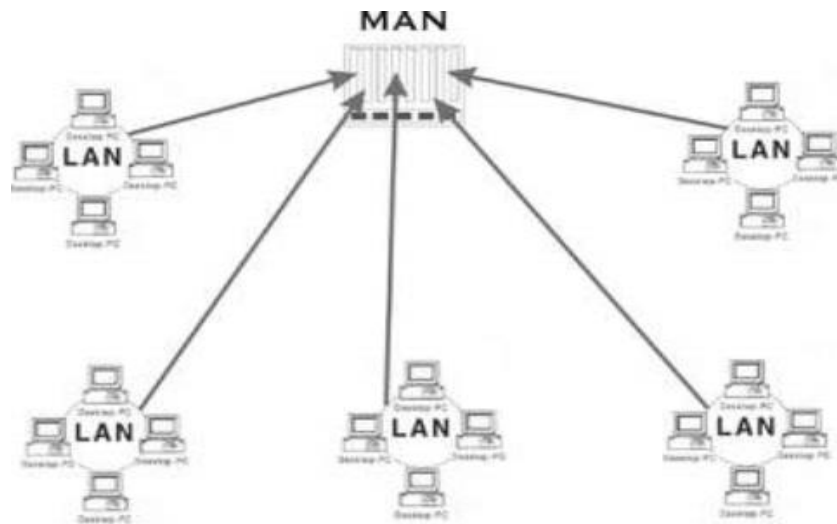


Figure 3 Metropolitan Area Network

- **(WAN) wide area network**

Any network covering a wide area, and connect local area networks with others is named as wide area network or (WAN). (WAN) may be used to connect some typical local area networks in an organization, or used by Internet service providers (ISPs) to provide a group access with Internet [10]. (WAN) are typically used of reduced lines [11].



Figure 4 Wide Area Network

2.2.1 Network Topologies

To linking many number of nodes with other in a computer network there are several possibilities. These possibilities are named as network topologies. The networks are designed by their importance and their purpose.

- **Line**

In a topology the nodes have 2 neighboring nodes at maximum. Data that has been converted from one end side to the other end side, will have to travel across the other line nodes [12]. This type of network topology is so easy to build, and it can extend for large distances because the line nodes will work as repeaters [12].

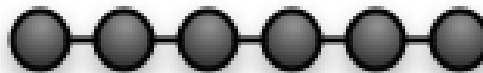


Figure 5 Line Topology

- **Bus**

In a topology of a bus the bus nodes are linked to a common medium. In the network every bus node is receiving the information that transmitted across that common medium, but just the node that the information are meant for, will accept the information. Other bus nodes, will in all the cases ignore the information. If a bus node fails, the network will receive data, but if the connection fails it can division the network, because there is no option route across the network [12].

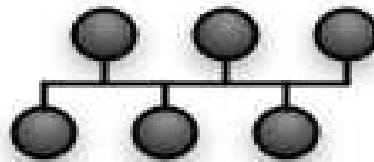


Figure 6 Bus topology

- **Ring**

All nodes in a topology are linked with the other nodes, this says that the network will build up a ring. But the ring is more expensive, and it leads to be inactive because it have to move across more ring nodes, then other topologies [12]. If one of the nodes fails it may effect on other nodes data transmitted, because in some applications the information are only transmitted one way across the network. It can then be considered as a line topology, with all its weaknesses. There is a very good way to solve this problem by using a dual ring topology, where each node has four branches connected to it. This makes the topology very good and prevent fail, but it also need more money [12].

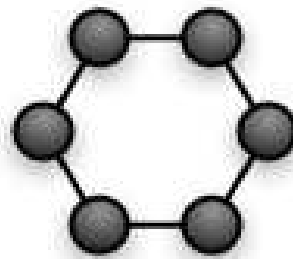


Figure 7 Ring topology

- **Tree**

In tree topology all founded nodes are placed like a tree. All the founded nodes are linked as tree leaves they are connected to other topology. But they have more cards of the network, and may be connect with other leaves. It's so important to know that no directive are done at the non leaf nodes, they just data information from its input to its output, such other node [12]. If a connecting to a leaf or the any node itself fails, it will only fail the leaf node. The network will be saved .But if a non leaf node fails, an entire section network will fail [12].

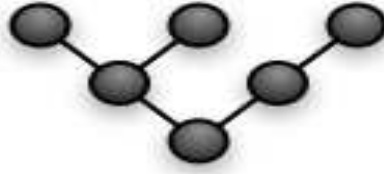


Figure 8 Tree topology

- **Star**

A star is a topology of the network that all the founded nodes are linked to a main center node. This main center node resend information that income to all the nodes linked to the main center node [12]. For a schematic acting of the star topology. When connection between any node and the main center node is broken, this will only isolating that node from the network and data will transmitted. But if main center node is broken, all the network will fail, and lead to isolating all the nodes [12].



Figure 9 Star topology

- **Mesh**

The mesh topology has two nodes at or more, with one or more tracks to other nodes. In mesh topology more wide area networks used, for example Internet. The mesh topology is a settlement between a fully connected topology and star topology. With a very good accuracy and a low connection cost, the mesh topology is the economical choice for (WAN) topologies [12].

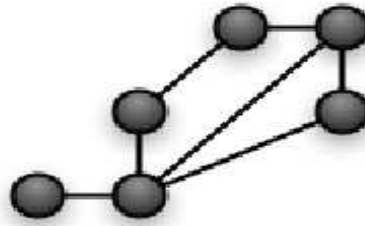


Figure 10 Mesh topology

- **Fully Connected**

In fully connected topology there are directly connection between all the founded nodes. This is the most redundant and a high reliability network founded, but this type needs more money because the direct connection is expensive in the cost to create and maintain [12].

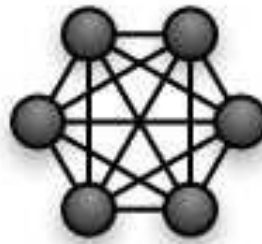


Figure 11 fully connected topology

2.2.2 Type of cables that used in networks

The type of wired cables are the main type of cables that used in every network topology and they are used for transfer data through networks, there are some types of cable that using in the networks.

- **Twisted Pair Cable**

The twisted pair electrical cable is the more common that used in all type of networks. It is created by using two cables around each other, this leads to reducing the crosstalk [7, 9]. The (UTP) cable, are used in telephone networks and computer networks.



Figure 12 Twisted pair cable

- **Coaxial Cable**

The Coaxial Cable used in some networks, named as coax, it is an electrical cable made from a round, insulated conducting wire, covered by an insulating spacer, covered by a cylindrical conducting sheath, usually covered by a final insulating layer [7, 9]. There are more type of the coaxial cable . In networking the thick (0.5, 0.25, inch diameter) [7, 9].

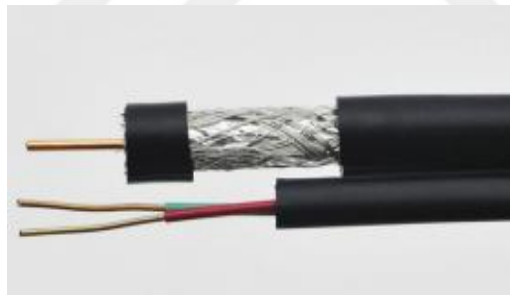


Figure 13 Coaxial cable

- **Optical Fiber Cable**

Fiber optic is a transparent superfine fiber used for transmission light. It made of plastic or glass, and fiber optic affected by electromagnetic interference, it used to work on data rates well in excess of those possible with other cables [7, 9].

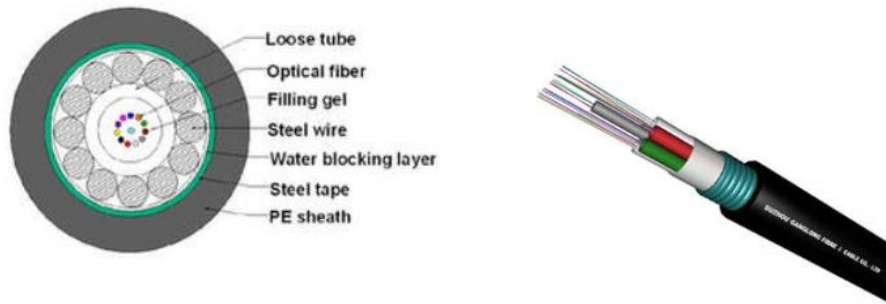


Figure 14 Optical fiber cable

2.2.3 Medium access control

Every networks are created by a transmission channel and a topology. But to take advantage of the structure, protocols and using standards and algorithms. There are more important medium access control for the networks standards are showed below:

- **Ethernet**

Originally the Ethernet is a frame that based on technology of computer networking for (LANs). The standard known was established wiring and signs for the physical layers, and the frame shapes and protocols for the (MAC) /the link of data layer of open system interconnection models. The Ethernet is especially unified as IEEE's 802.3, and it bearing the networks traffic at rate of 10 Megabit per second (Mbit/s) [7, 8].

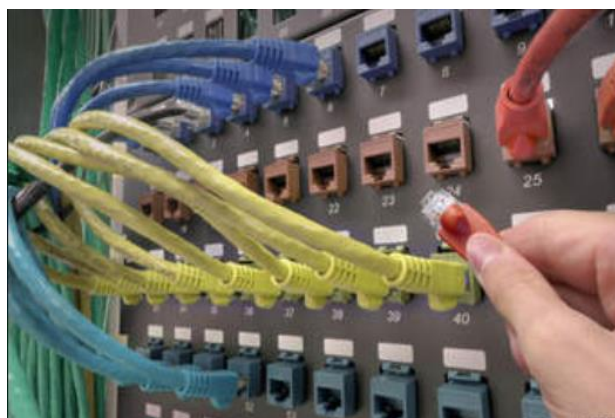


Figure 15 Ethernet cable

- **(FDDI)**

Fiber-distribute data interfaces are standard formats for transfer data in a (LAN) that can expansion up to 200 km by using a topology that is a dual attached model [13].

- **(PPP)**

Point-to-Point Protocol is used to make a direct link between nodes in a network. Its basic use to connecting computers by using a phone line [13].

- **(ATM)**

Asynchronous Transfer Mode is a cell follow up network protocol that do encryption on data traffic into a very small fixed sized (53 byte) cells allowance of changed sized packets as in packet switched networks(like the Internet Protocol or Ethernet)[7, 8, 12].

2.2.4 Network Protocols

There are some several protocols in use in a typical network model. The Internet protocol suite is the most known protocol.

- **Internet protocol suite**

Internet protocol suites model is a group of telecommunications protocols that apply the protocol package on which the Internet starting to work. It is named as the TCP/IP protocol suite, after the two more important protocols in the Internet protocol suites: (TCP) and (IP) [12, 14, 15].

- **(IP)**

Internet protocol is a data information directed protocol model used with a source and intended devices for connecting data as a packet-switched internet work [15]. Information in an IP are sent in datagrams or blocks pointed to as packets or datagram's. In especially no setups are wanted before a device tries to send datagrams to a device it has before not connected with [11].

- **(TCP)**

A (TCP) is a model of a communication directed and trusted connection byte flow transfer. It does the mission of the transfer layer in the simple OSI type of the networks. In TCP model there is guaranty for message connecting [13, 15].

The connections of transmission control protocol contain are:

- 1- Enterprises
- 2- Information transfer
- 3- Connection ending

The three way handshake model is used to proof a connection. And the other way named four model is used for tear down connection proof, the standards like sequence numbers or other things are configured to help guarantee command connection and durability [11, 12].

- **(UDP)**

The User Datagram Protocol (UDP) is a protocol as a less message directed transfer layer. In the TCP/IP model, UDP offer a very easy link between the network classes below and the application layer above. In UDP model there is no ensure for message connecting and a UDP sender keep no state on UDP messages once sent onto the network it cannot used in live applications. UDP adds information check summing on head of an IP data [12, 16].

2.3 Electrical Networks

Electrical networks are the correlation between the electrical elements like, or a model of correlation, consisting of electrical elements. And they are closed loops, and give a back path for the electrical networks, an electrical network type only have one type of sources (voltage or current) [17, 18, 19].

2.3.1 Electrical circuits types

Types of electronic circuits:

- 1- Series
 - 2- Parallel
 - 3- Series Parallel (combination of both series and parallel).
- **Series**

The series has two or more resistors (any element that using electricity to in working), they have moving on one direction for charges. Charges should have moving in series in the beginning time it must to charging one resistor and then charge the next. In the case one of the circuit elements is broken then charge will stop moving.

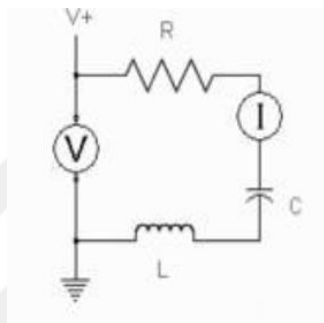


Figure 16 Series Circuit

- **Parallel Circuit:**

The parallel circuits have two or more resistors (anything that using the electricity to do work) and they there are several tracks to moving along .The charges can moving across any one of several tracks. If any elements in the circuit is failed then no charge will move across that tracks, but other tracks that not failed will continue to have charges flow across them. There are more Parallel electrical wiring.

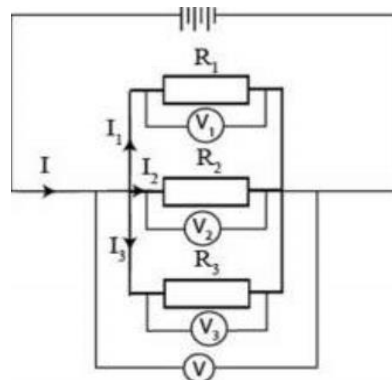


Figure 17 Parallel Circuit

- **Series Parallel Circuit:**

This type of circuit is a collection of both series circuit and parallel. The electric current travels through both series circuit and parallel circuits.

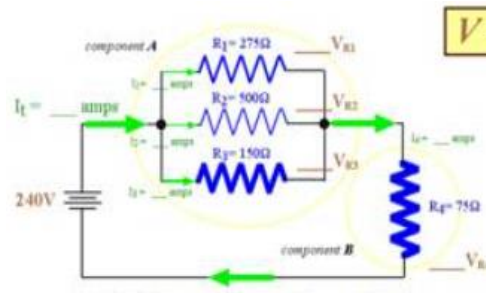


Figure 18 Series Parallel Circuit

2.3.2 Planning and Reduction the Cost for the electrical networks

Increasing of demands are published on new hospital buildings. In the starting from planning, wanting for a very high level of security and flexibility in our life, a low level of environmental contamination, the merger of renewable network for the designer and the way to minimizing costs must be taken into the accounts in order to investment the full possible of economic events and investigation technical requirements must be taken in building hospitals [20, 21].

Various concepts associated with buildings and developments are defined as follows:

- 1- The building properties, developments of the outdoor facilities, engineering structures, transportation installations, load-bearing structures, and technical system equipment
- 2- The new structures and new installations, represent properties which are newly constructed or set up.
- 3- The extensions, represent new models additions to an existing property.
- 4- The maintenance work represents steps taken to retain the designated condition of a property.
- 5- Modernizations represent structural steps taken to sustainably increase the practical value of a property.

- 6- Renovation refers to steps for restoring the originally intend condition (designated condition) of a property.
- 7- The enclosing space developments refer to the inner design or set-up of interiors without significant incursions made into the substance or structure.

2.3.3 Basic Consideration on Power Distribution

Electric power supply is the most important task for the stage of establishing basic data estimation of power required for any supply. In order to attain a high efficiency, the components should work with a load between 70 to 80 % of the maximum power output. Under sizing causes malfunctions, while oversizing results in excess costs [19, 22]. Configuration of the network and its power distribution is determined and depended on the requirements resulting that use. Like the specifications that made by the installation designers and the intended use of the electrical network in hospital building, the required power output must be distributed between different sources of supply. If redundancy is a system requirement, an additional reserve must be considered in the planning. Besides the demand to be met by the normal power supply (NPS), the power required from a safe and reliable source of supply must also be very good estimated. The safety power supply (SPS) demand is divided between the emergency standby power system (ESPS) and the uninterruptible power supply (UPS). When the NPS fails, the UPS must be supplied from the ESPS. In addition, the power demand of safety equipment.

2.3.4 Electrical Power Distribution Systems Drafting in electrical network

Requires that integrated solutions of electrical power distribution. Totally Integrated Power (TIP) provides support in working out suitable solutions. This consist of software tools, support for planning, configuring, perfectly harmonized, complete portfolio of products and systems for integrated power distribution, ranging from the medium-voltage switchgear to the final circuit [23].

With TIP renders support to meet requirements such as:

- 1- Simplification of operational management by a simple network topology.

- 2- Low power losses, by transmission the power of medium-voltage-side to the load centers.
- 3- Good reliability of supply and safety of operational of the installations.
- 4- Changing load and operation by easily conditions.
- 5- With friendly equipment make Low operating costs.
- 6- The equipment transmission capacity of under normal operating conditions and under fault conditions.
- 7- A good quality of power supply that meaning a few voltage changing due to the load fluctuations with sufficient voltage symmetry and low harmonic distortions in the voltage.

2.3.5 Supply and operating Voltages in Distribution Grids

Different voltages are used in different tasks of electric power supply and distribution. In electrical networks there are two voltage groups:

- 1- Medium voltage (MV): more than 1 KV, AC up to 69 KV AC.
- 2- High voltage (HV): more than 100 KV, AC up to 230 KV.
- 3- Low voltage (LV): up to 1,000 V, AC.

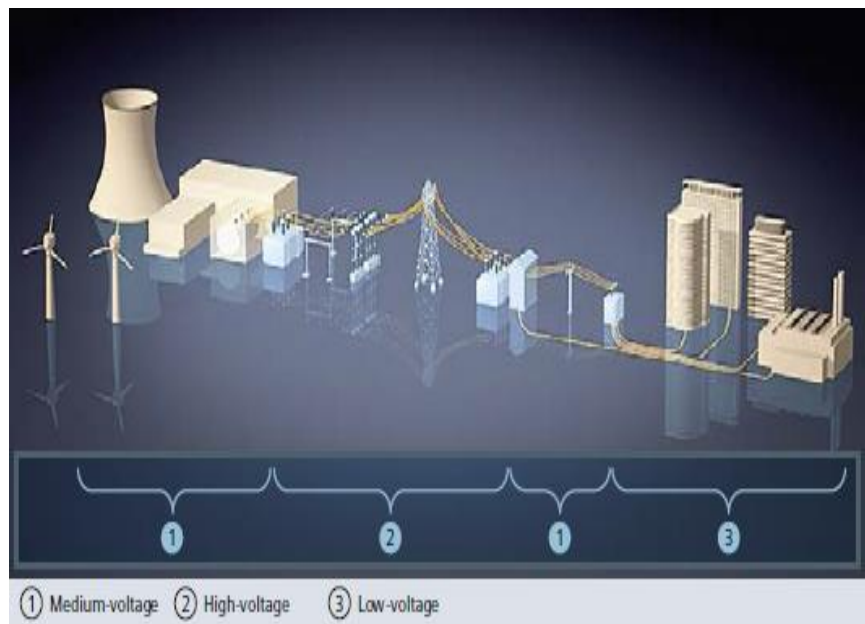


Figure 19 Voltage levels between the power station and the consumer

2.3.6 Type of Power Supply

Electrical energy can be fed into the grid in different ways, determined by its primary function. For normal power supply (NPS):

- 1- Transfer from the medium-voltage grid (max. 33 kV) via public.
- 2- One or more generators for general standby operation and / or safety power supply (SPS).
- 3- UPS, Uninterruptible power systems for some parts.

a: The model of static UPS comprising a rectifier or inverter unit that have battery or fly wheel energy storage for buffering voltage failures.

b: The model of rotating UPS comprising a motor or generator set that have flywheel energy storage or a battery plus rectifier or inverter unit for bridging.

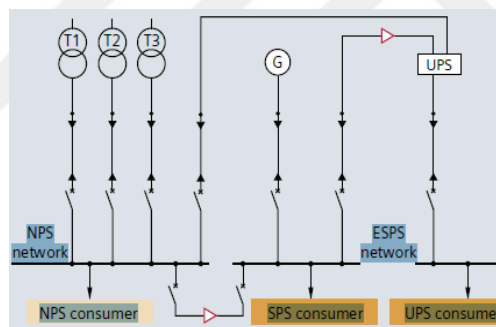


Figure 20 Type of power supply

2.3.7 Network Configurations

From the type of the supply we can distinguished the electric power distribution grids or networks according to the type of meshing.

The following basic configuration are distinguished:

- 1- The radial networks
- 2- The ringed networks
- 3- The meshed networks

The simplest form is the spur line fed radial network. The advantages lie of protection and the fast fault localization and simple operational management. In the time of the doubled, the outcome is a double spur network. Every load center can be reached via two different paths. The switching devices are only closed if required. If the requirements placed on supply reliability are high, each supply line can be fed from an independent supply network. Due to fact that the networks are independent from each other, if a fault accrue in one network will not affect the other one.

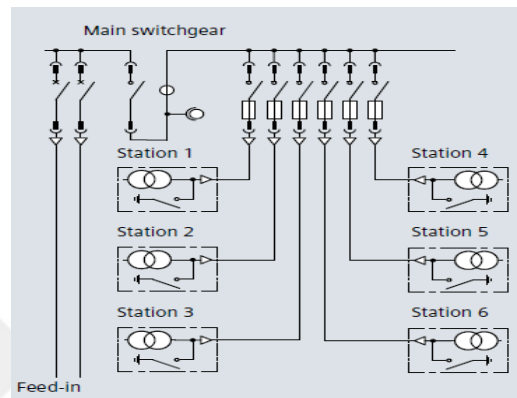


Figure 21 Radial network

As an extension of the spur network the ringed network in combination with a ring line can be built up. With dependent on spatial structures, the investment can make for an open type ringed network and can be lower than or higher than of the spur network. The spur network is advantageous if the transformers shall handle with low voltage supply in a confined space. The ringed network are favorable regarding costs of investment if supply is spread out over a larger area with several transformer centers. With the space requirements, power demand of the coverage, environmental lines and cable costs, the differences between the two network configurations are low [23]. And ringed networks are more than often come with shorter cable lengths, the cable cross sections must be higher than the owing to the transmission of the higher capacities from the one ring endpoint to the other. The costs of the power losses, the spur network and the open type ringed network only different in insignificantly. There are minimal advantages if the ringed network is operated in the closed type variant. However the protection of the closed ring requires circuit breakers and line differential protection. These additional costs are not small in investments.

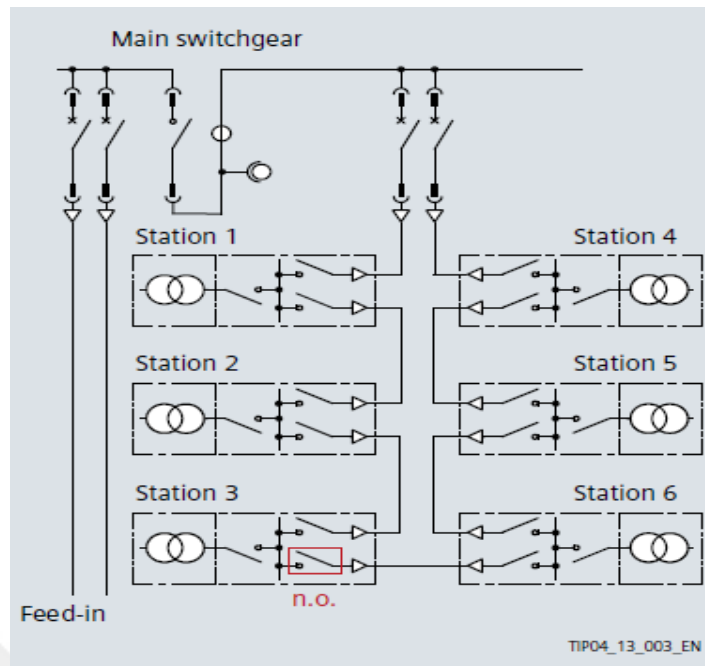


Figure 22 Mesh network

If a fault occurs in an open type ringed network, all the stations downward of the fault location up to the normally open switch will fail. With the case of low voltage side meshing of the ring stations, the failure of a large sub ring could result in overload and disconnection of non-affected, still operable transformers. If a cable fault occurs in the spur network merely results in the failure of one station. With a closed type ringed network and a good protection expense could like a level of reliability be also attained in the ringed network only. In addition with the closed type ringed network provides an immediate reserve if a cable fault occurs, whereas the spur network merely offers a load transfer reserve. A single fault with transformer failure can be handled in both networks without interruption.

2.4 HIS

A hospital information system (HIS) is an item of health information system that concentrate basically on the management the required information in hospitals. In many applications, a HIS is an inclusive complete information system designed to administration all the sides of a hospital's operation, such as medical, administrative, financial, and legal issues and the corresponding processing of services [24, 25, 26].

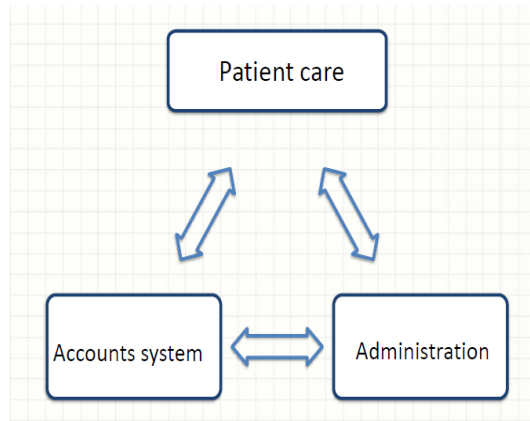


Figure 23 Hospital information system

2.4.1 Patient care

Patient care means the followings:

- 1- Patient registration.
- 2- A special number for the patient.
- 3- Information about the patient and previous cases.
- 4- Diagnosis of the disease and his medicine.
- 5- Registration of laboratory.
- 6- Registration of X-ray.
- 7- Registration of notes.
- 8- Reports and information summary.

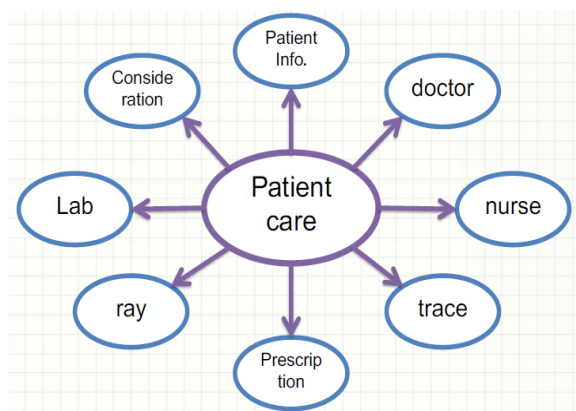


Figure 24 patient care

2.4.2 Administration

Administration means the followings:

- 1- Medications and hospital use of existing ones.
- 2- Report in the form of (daily, weekly, monthly ...) for the use of existing materials [27].
- 3- Hospital pharmacy.
- 4- Control of drug stores: input and output movement.
- 5- Returns the items expired and corrupt.
- 6- The sale of medicines.

2.4.3 Account system

Account system means the followings:

- 1- Hospital File records.
- 2- Accounts (daily, weekly, monthly ...) for the Hospital needs and rights and the economic situation expenses [28, 29, 30].
- 3- Report in the form of (daily, weekly, monthly ...) for the Hospital Incoming.

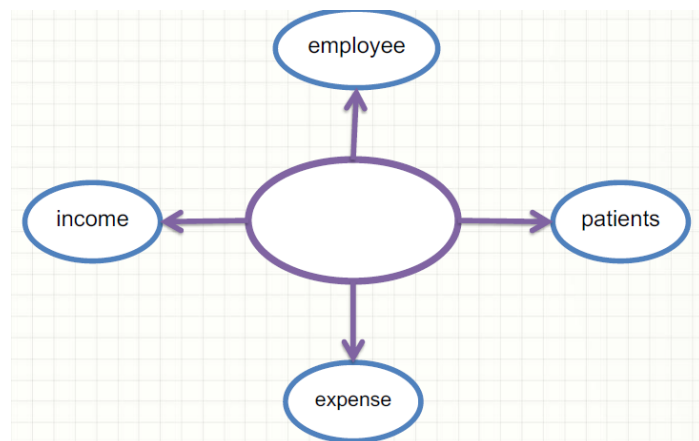


Figure 25 account system

2.5 Some monitoring programs

1- Cacti

Cacti is a complete, web-based network graphing solution designed by features to harness the power of RRD tool's data. It reconnaissance network switch or router interface services via simple network management protocol at predetermined intervals and graph the resulting data. It capable of graphing resulting data of hundreds devices or small number of network devices. Depending on the data stored on RRD tool graphic database, Cacti working to build up of reports in numerical and graphical forms. Also it includes user management features, allowing administrators to find users and relative permissions.

2- Multi Router Traffic Grapher (MRTG)

The Round Robin Database Tool is a program that records and imagined digital data in an efficient manner. The RRD Tool is a key component of the next major release of the Multi Router Traffic Grapher (MRTG). It is already fully implemented and working. Because of the massive performance gain possible with RRD Tool some sites have already started to use RRD Tool in production. The original MRTG program was a Perl script which used external utilities to do SNMP queries and to create GIF images for display on the HTML pages. MRTG logged its data to an ASCII file, rewriting it every five minutes, constantly consolidating it, so that the log file would not grow over time.

3- WIRESHARK network analyzer

Wireshark is the network protocol analyzer that lets to see the inspection of many types of protocols, on the network at a microscopic level. Runs on Windows, Linux, and many others platform and operating systems. Apply many type filters on Live captured values and display it on screen or Output can be exported to XML, CSV.

CHAPTER 3

SYSTEM ARCHITECTURE

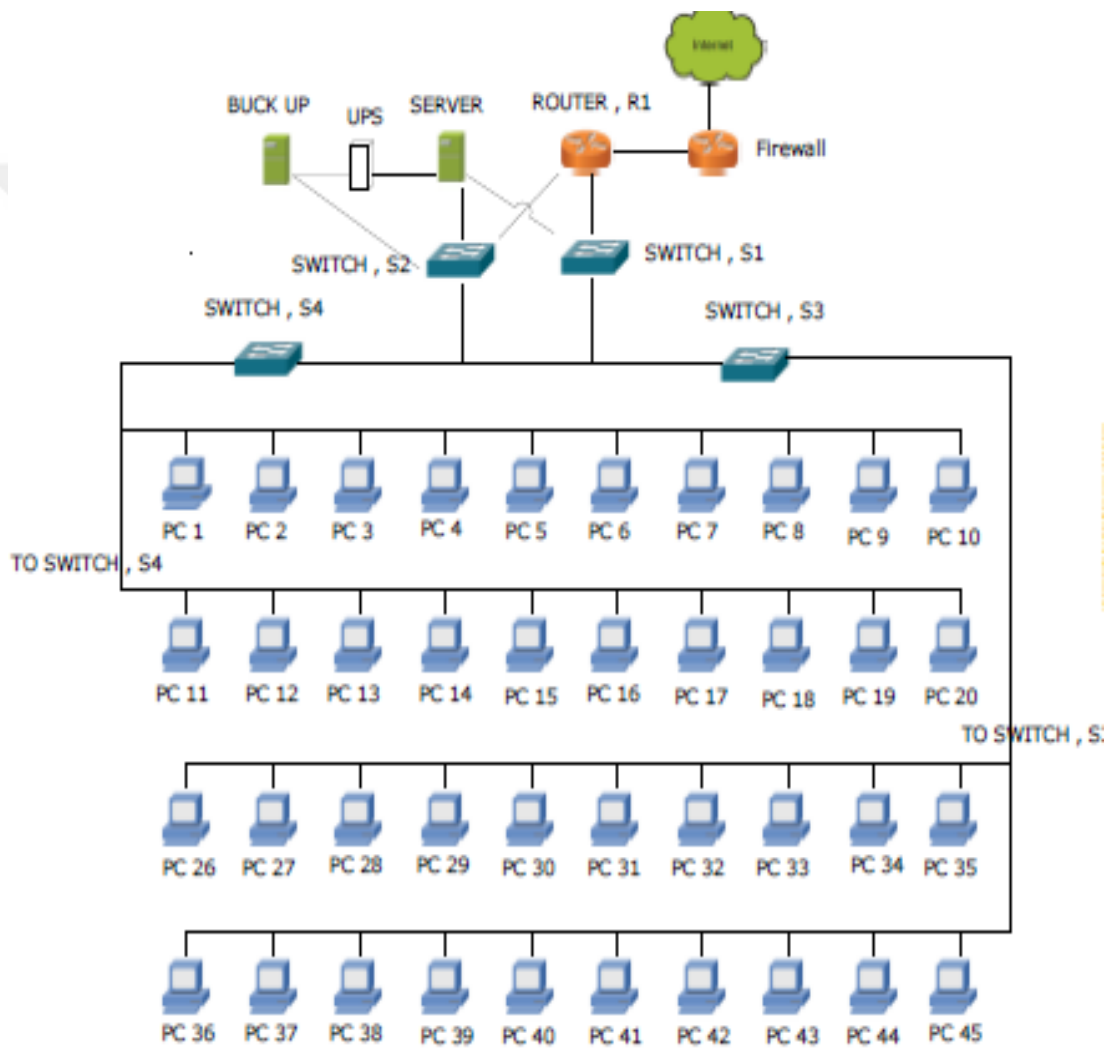


Figure 26 system overview

3.1 Overview

An overview of the different devices forms in the system is given in figure 26. The system consists of the main entities: Router, Firewall, Server, and Backup server, UPS, 4 Switch, and 40 Clients, 20 for first floor and 20 for Ground floor, the Clients 21, 22, 23, 24 and 25 are spare numbers for adding in the future if needed. The system is quite independent because this is a combined system we can use this system inside a hospital without connecting with internet and we can connect to internet. This system is designed to implement a hospital information system as a database that may be designed. In this system we can use internet protocols and wired security inside hospital and wireless security when we connect to internet and using firewall to add new security to the system. This system is ready to connect with other places or hospitals for example with ministry of health in the future.

3.1.1 User

- The basic user: is the person who is able to use his own user name and password, and he is working inside the hospital. He may be a doctor or nurse or anyone, but he can only enter information and connect with other parts inside the hospital and receive information from database server.
- The advanced user: is the person who is able to use his own user name and password, and he is working inside the hospital. He can enter the database information and connect with other parts inside and outside the hospital and receive and send information from and to database server.

3.1.2 A Client

A client is an element used by a person to participate in the network or to access the Internet. Three types of clients are specific for using in the networks: desktop, laptops and handheld. Now laptops are the most common client used with networks. But this will change in the future with new devices [31].



Figure 27 type of clients

3.1.3 Switch

The switches at layer 2 are high speed very smart bridges, have multi ports, switches process frame in hard ware through the use of application specific integrated circuits. Switches have the following features:

- Bbackplane with high speed: The circuit allows the switch to monitoring multiple conversations that increases the network speed.
- Data buffering: A buffer is a memory storage .This thing allow the switch to store frames and forwarding them to the port.
- Higher density of port: Density of the port is the number of available ports on a single device. Some switches can have more than 100 ports.
- High speeds of port: The good device can support a mixture of port speed from 10Mbps to 10Gbps.
- Virtual LANs (VLAN): switches can with logic segment the networks into separate broadcast domains.

The following primary frames switching modes exist:

- Cut-through: Cut-through: To check of the distention title and for directly starting redirection the frame this can reduce time.
- Storing and forwarding: The switch want to getting the complete frame before redirection ,while reading the getting and a cycle reducing check is operated. The meaning of bad (CRC) is discrete frame.

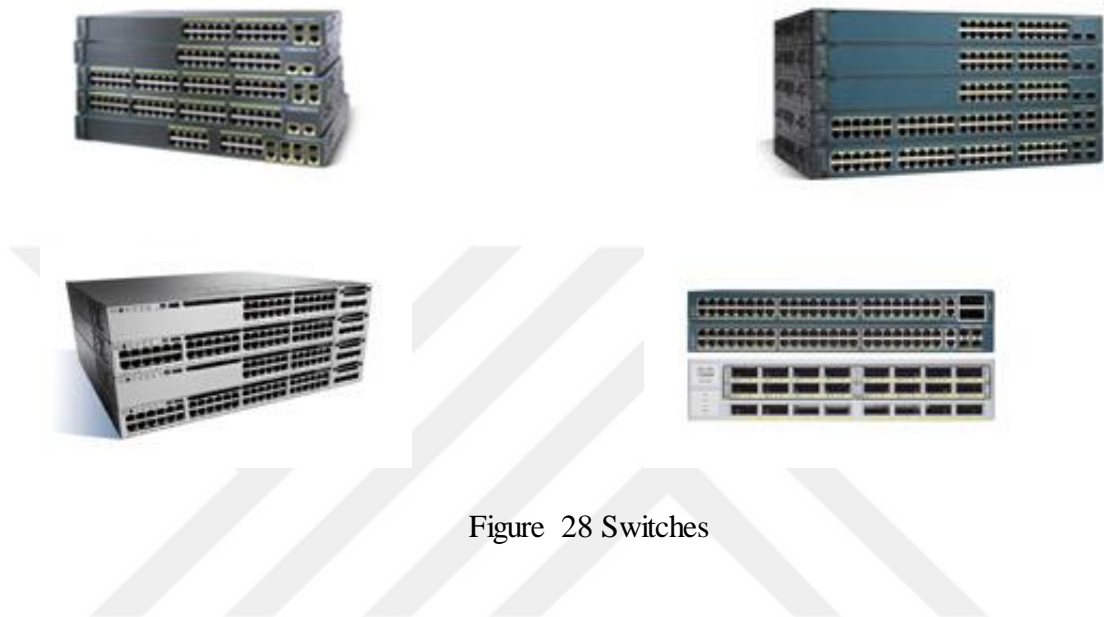


Figure 28 Switches

3.1.4 Cost analysis for different brands of switches

There are more brands of switch and more type of switches, which can used in networks. But every brand and type has different price that make the engineers or designers to thinking about the cost to build and design a network. In our design we used 48 port and 24 port switches and we need to know the available brands and the prices of every brand and every type we need.

The following are some brands of switches and there prices:

- **HP Switches**

- 1- J4899C ProCurve Switch 2650 48 ports 10/100 and 2 dual personality ports each port can be used as either and RJ-45 10/100/1000port or an open mini-GBIC slot. **823 \$**

- 2- J8161A HP ProCurve Switch 10/100-TX Mod 24 port IEEE 802.3 ready module for the 5300 switches. Used with the 600 or 610 EPS, the module provides Power over Ethernet. **2,299\$**
- 3- J8706A ProCurve Switch zl 24p Mini-GBIC Module 24 port mini0-GBIC zl module for the ProCurve 5400zl series switches. **4,169\$**

- **Cisco switches**

- 1- Cisco Catalyst Switch WS-C3750X-48P-E, 48 GE Port, PoE, IP Services, Stack Wise Plus, Stack Power, Energy Wise, MACsec, investment protection. 8,712\$
- 2- WS-C2960X-48TS-L. 4 x 1G SFP, LAN Base. 1,469 \$
- 3- Cisco 3750-X Switch WS-C3750X-24P-E Catalyst 3750X 24 Port PoE IP Services. 4,680 \$
- 4- Catalyst 2960-X 24 GigE PoE 370W, 2 x 10G SFP+, LAN Base. 1,609 \$

- **Huawei witches**

- 1- New 100% Original Huawei S5700S-52P-LI-AC 48 Gigabit Smart + 4SFP Switch. **800\$**
- 2- For HUAWEI S5700-24TP-SI-AC 24 enterprise gigabit switch Products Status: Stock; Function: Stackable; Function: VLAN Support; Ports: 24Transmission Rate: 10/100/1000Mbps. **680 \$**
- 3- Huawei SmartAX MA5626-8 MA5626-16 MA5626-24 with 8 ports 16 ports 24 ports IP Dslam network switch(China (Mainland)) Huawei SmartAX MA5626-8 MA5626-16 MA5626-24 with 8 ports 16 ports 24 ports IP Dslam network switch. **388\$**
- 4- Huawei MA5620-24 fiber switch, GPON or EPON terminal ONT with 24 Ethernet and 24 voice ports apply to FTTBBrand Name: HUAWEI ; Model Number: MA5620-24. **200\$**

- **H3C switches**

- 1- (China (Mainland)) H3c switch ls-5500-52c-ei kilo mega 48 Products Status: Stock; Transmission Rate: 10/100/1000Mbps; Ports: ≥ 48 ; Function: VLAN Support; Function: Stackable. **2,954 \$**
- 2- H3c ls-s5120-52c-ei-h3 48 gigabit managed switch s5120-52c-ei

Products Status: Stock; Transmission Rate: 10/100/1000Mbps; Ports: ≥ 48 ;
Function: VLAN Support; Function: Stackable. **1,994 \$**

- 3- (China (Mainland)) H3c ls-s5500-24p-si gigabit switch 24 network switch enterprise Products Status: Stock; Transmission Rate: 10/100/1000Mbps; Ports: 24; Function: VLAN Support; Function: Stackable. **1,187\$**
- 4- H3c ls-3100v2-26tp-si 24 Ethernet switch 24 switch Products Status: Stock; Transmission Rate: 10/100/1000Mbps; Function: VLAN Support; Function: Stackable; Brand Name: None. **307 \$**

When you read and know the types and prices of switches that shows us the importance of knowing the network that we want to design. We know that each type has its own advantages and disadvantages, but is it important to know what we want, because every device means more cost. So cost and type of every devices is very important.

3.1.5 Router

A router is using to find a path to a destination and moving data across this path to the destination. The process of routing using the table of routing, and the algorithm to determining the effective track of the IP packets forwarding.

The following are the key functions:

- Path determination: The packets of routing tables and network address are transmitted through the network. The routing process includes through the network determining the optimum path. By using the routing protocols the router can communicate the network information from the router's own routing table with neighbored router's.
- Packet forwarding: After determining the path, the forwards a packet through its network interface toward the destination.



Figure 29 Routers

- **Routing Versus Routed**

Network layer protocols are routed protocols or routing protocols. These are defined as follows:

- A routed protocol: The network layer protocol that provides information within its address to allow the packet to direct User traffic. Or determines the address shape with using the area in the packet Routed protocols include IP, AppleTalk, and others.

- Routing protocols are able to determine how routed protocols are used by:

- 1- Providing mechanisms for sharing routing information.
- 2- Allowing routers to update each other about network changes.

- **Path Determination**

Network addresses and routing tables transmit packets through the network. This process of routing includes determining the optimum path through the network and moving the packets along the path [38, 39, 40]. A router can use the following types of entries in the routing table to select the best path:

- Static routes; Entered routes in the routing table manually.
- Dynamic routes: Routes learned from a routing protocol dynamically.
- Default routes: The static or the dynamic route that tells the router where to route packets not explicitly in router.

- **Routing table**

In this type of routing all routers are learning about all the routes founded and storing this information in the routing table. A router are learning about itself in these three ways:

- Direct connected networks.
- Statically (the network administrator entered all routing information).
- Dynamically (in the network a routing process running) the information stored in a routing table includes destination/next-hop and routing metrics. Destination/next-hop tells the router whether the destination is directly connected or is available through an adjacent router.

- **Dynamic Routing Protocols**

Routing metrics are measures of path desirability. Different metrics use different protocols. The common metrics are as follows:

- Bandwidth: The capacity of data links.
- Delay: The needing time to transfer the packet from the current router to the destination. This process depend of the band-width of the medium connecting, the port delays time.
- Load: Activity of amount on the network.
- Reliability: The rate of error in every network connecting.
- Cost: A value of an arbitrary based on, expense, bandwidth, and other metrics assigned by the person who administrate the system.

- **Routing Methods**

The designing of protocols of routing are about one of the followings:

- Distance vector routing: It is an updating method that called "routing by rumor" All routers receive updates from them direct neighbors [36, 37].

- Link state routing: that means how they interconnect together. The network information's are shared in the forms of link-state advertisements (LSA). Link-states muting provide:

- 1- Link-states send only topology changes. Distance vectors send complete routing tables.
- 2- Link-states updates.
- 3- Link-states use the two-state hierarchy (areas and the systems that autonomous), which limit change.
- 4- Link state supports summarization classless.
- 5- Link states muting converges fast and are robust against routing loops, but they require a great deal of memory and strict network designs.

- Advanced distance vector: Collecting both link state and distance vector protocols. Use distance vectors with more accurate metrics, but deferent with the distance vector routing protocols an example of it is Cisco Enhanced IGRP (EIGRP) [32, 33].

3.1.6 Firewall

A firewall is a device used for security of the network, with hardware device and software programing based, that shows and controls inner and outer traffics that depended on some of rules. Behave as a wall between a reliable network and other unreliable networks such as the Internet [34, 35].



Figure 30 Firewall

3.1.7 Firewall types

1- Hardware

Some examples of hardware firewall ;(cisco pix. Net screen. Watchguard. Etc...). But this type is more expensive.

2- Software

It is easy install and don't need physically space and it is cheap.

3.1.8 Firewall techniques and details

1- Packet filter

It looks at each packet coming or going out of the network accepting or rejecting based on user rules.

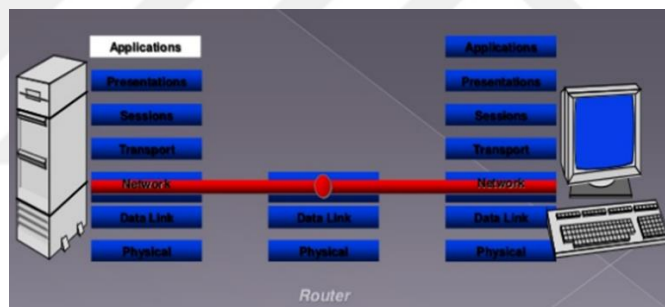


Figure 31 Packet filter

2- Application gateway

In this type of firewall network can interact only with proxy server.

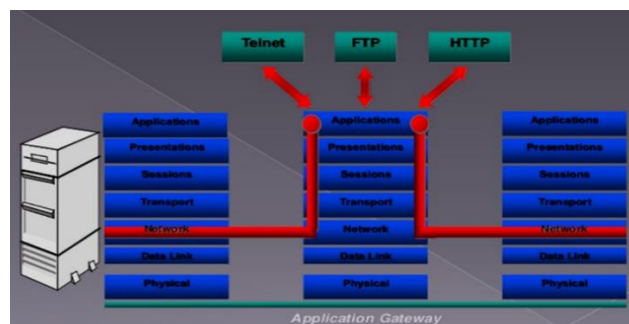


Figure 32 Application gateway

3- Circuit-level gateway

It is a standalone application. It sets up two TCP connections.

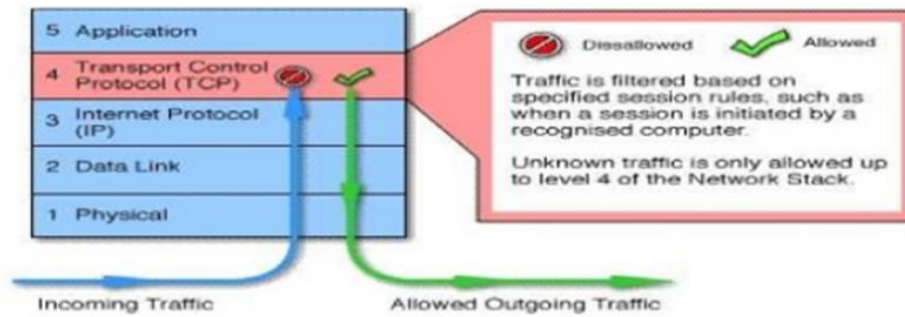


Figure 33 Circuit level gateway

4- Bastion host device

It is designed and configured to withstand attacks.

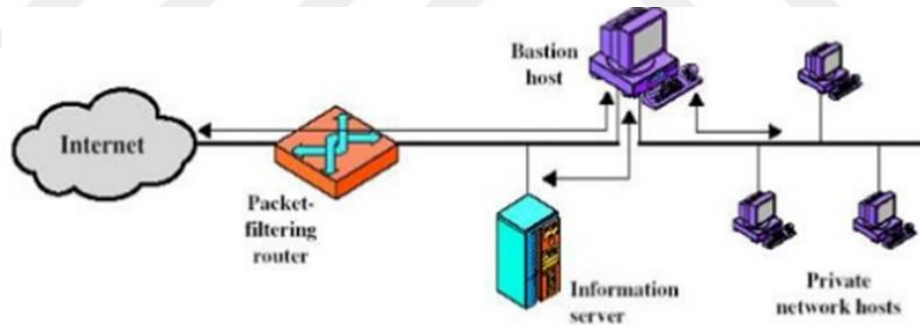


Figure 34 Bastion host

CHAPTER 4

ELECTRICAL REQUIREMENTS FOR A HOSPITAL

The Office of Statewide Health Planning and Development (OSHPD) is responsible for enforcing all building standards, codes, and regulations pertaining to health care facilities in this case.

The following document was compiled by the OSHPD electrical engineering staff as a guide for review of the plan to verify compliance and is intended for OSHPD use. It highlights and summarizes the most common requirements encountered in the review of a hospital.

4.1 Review of the Plan

The following are working as a guide for electrical requirements that can be used in hospital planning.

- 1- All plans of electrical and specifications must be signed by the electrical engineers or supervisor of records.
- 2- It must use a list of symbols and abbreviations used on plans that are used in the hospitals and their meanings.
- 3- Right electrical codes and version must be used.
- 4- The name of rooms and number of all plan sheets.
- 5- A plan of site that showing all the electrical locations.
- 6- A schedule showing the feeders, phases and earthen systems conductors, the sizes of the conduit, the lengths that are estimated for conductors, and overcurrent protective devices.
- 7- Locations and the sources of the power for all devices that are wired, including wires, lights, switches, junction boxes, outlets of power, and outlets of telephone, computer networks outlet.

- 8- The nursing call system. Provide equipment's specifications, showing location of all devices, and power source connection.
- 9- Providing a fire alarm system. With all elements for the hospital.
- 10- All hardware must be labeled, listed.
- 11- Schedules of ratings of electrical connection ratings of equipment requiring it.

4.2 Electrical system

Electrical system consist of system separation, service equipment, mechanical and electrical rooms. And all requirements of the system are:

- 1- Electrical system consist of all the requirements of the system that includes the kind of the equipment and the emergency system.
- 2- At least, we need 3 switches and we need also 1 transfer switch for every branch. And we need just 1 for full demand.
- 3- We need independent branch wiring for all the wiring systems.
- 4- Services must be stems or passing across existing facilities.
- 5- Ability of the load materialization wanted for all adaptation to existing systems.
- 6- One minimal lighting at least in electrical and one minimal lighting at least in mechanical rooms.
- 7- Protection of the fault of ground needs on main circuit breaker and feeders if supplied on main.

4.3 Emergency power system

Emergency power system consist of generator, alarms, fuel supply, and transfer switches. And all requirements of the emergency power system are:

- 1- One generator or more must be founded as an alternate source of power.
- 2- Battery charger must be founded at generator set and charger for automatic starting.
- 3- Selected plugs at generator set and transfer switch locations.
- 4- The time of automatic restoration of power must be less than 10 seconds.
- 5- The fuel supply for at least 24 hours must be founded on site of operation.

- 6- Visual, audio alarms must be founded to show generator operating, the temperature of water, oil pressure, 6-hour fuel needs for generator and charger case.
- 7- Using (ATS), automatic transfer switches bypass and isolation capability.
- 8- Separator four (4) pole transfer switches grounding systems required.
- 9- Over load protection and over voltage protection required.
- 10- Generator set accessories and separate generator room required.

4.4 Conduit and wiring

Conduit and wiring needs materials and installation that used in some places, and the requirements are:

- 1- For fire alarm system, nurse call system, communications systems and computer network we must using low voltage cables.
- 2- The wiring for emergency system must be taken in solid metallic raceway.
- 3- The plastic tube may use for tunnels, emergency, for inside or outside wiring of the building. It is forbidden to allow for branch circuits supply service to patient care region.
- 4- Non solid metals raceways and metals sheathed cables are allowed in the following:
 - a. precast medical head walls.
 - b. furnishings.
 - c. on the places that not damages.
 - d. connection with non-solid equipment.
- 5- All wiring linked to the emergency and all light switches must be identified in a clear style such as with colored plates or colored devices.
- 6- The wiring in patient care areas should be characterized.
- 7- Rooms, sub ways must be industrial lighting.
- 8- Lamps must be protected against accidental breakage.
- 9- To prevent short circuit, we need mathematical calculations of overload protection sized for locked rotor amps.

4.5 Communications and signal systems

This systems consist of some parts like:

- 1- Emergency fire alarm power, the system consist of smoke detection, control panel, and electric water flow.
- 2- Nurse call power on emergency.
- 3- Medical Gas alarm power.
- 4- Using the system of communication for issuing instruction during emergency conditions.

4.6 Non-patient area branches needed

The non-patient area divided to: Clean Utility Rooms, Solid Rooms, Blood Bank, Laboratory, Telephone Equipment Room, Nurses Station, Network and information Technology Equipment Rooms, Pharmacy, Corridors, Exits, Entrances, Kitchen and restaurant, and the requirements are:

- 1- For control in emergency illumination we need one or more egress switches.
- 2- The exiting signs illumination.
- 3- Laboratory hoods on emergency that used fume.

4.7 Patient area branches needed

The patient area divided to: Patient Bedroom, Isolation Room, Pediatric Locations, C.T. Scanner, X-Ray, (MRI), Birthing Room, Nursery, Neonatal Intensive Care Unit (NICU), Delivery Room, Emergency Room, (ICU), (CCU) and the requirements are:

- 1- Two (2) number of separate branch circuits and Two (2) number of dual hospital grade plugs per bed.
- 2- All plugs tamper resistant in children locations.
- 3- We need nurse call point per bed, WC, bath.
- 4- Task illumination on emergency.
- 5- Emergency lift.
- 6- Some portable devices worked by 110 volt.

- 7- Connecting all devices to the grounding.
- 8- Because there are strong magnetic fields linked with this devices that used in some places, it should followed the recommended. There are some of the acceptable recommendations.
- 9- Emergency battery powered lighting units should be used in delivery rooms.
- 10- Surgical light.
- 11- Standard clock which is direct wired or battery operated.
- 12- Using Isolated power systems.
- 13- Pale or multi-level switching per bed area lighting should be used in (ICU) and (CCU).



CHAPTER 5

ENFORCING NETWORK SECURITY BY CONFIGURATIONS DESIGNED MODEL

5.1 Introduction

The Switches, Routers, IPS and Firewall are some of equipment's that work widely to equip security for network system devices such as PC

5.2 Configuration of external sources

An IOS device can be configured from the following external sources:

- 1- Console terminal
- 3- Remote terminal (aux port)
- 4- Telnet
- 5- Cisco Works
- 6- SSH

To initially configure a router or switch, only console connection or remote terminal connection can be used.

- **Console Connection**

To do a connection through a console port, you must have a swaddle cable that uses to link a console port to your computer. For set up the linking, follow these two steps:

Step 1. Connect your instrument using a swaddle cable. If Your PC does not have console way you must use an adapter.

Step 2. Configure the device.

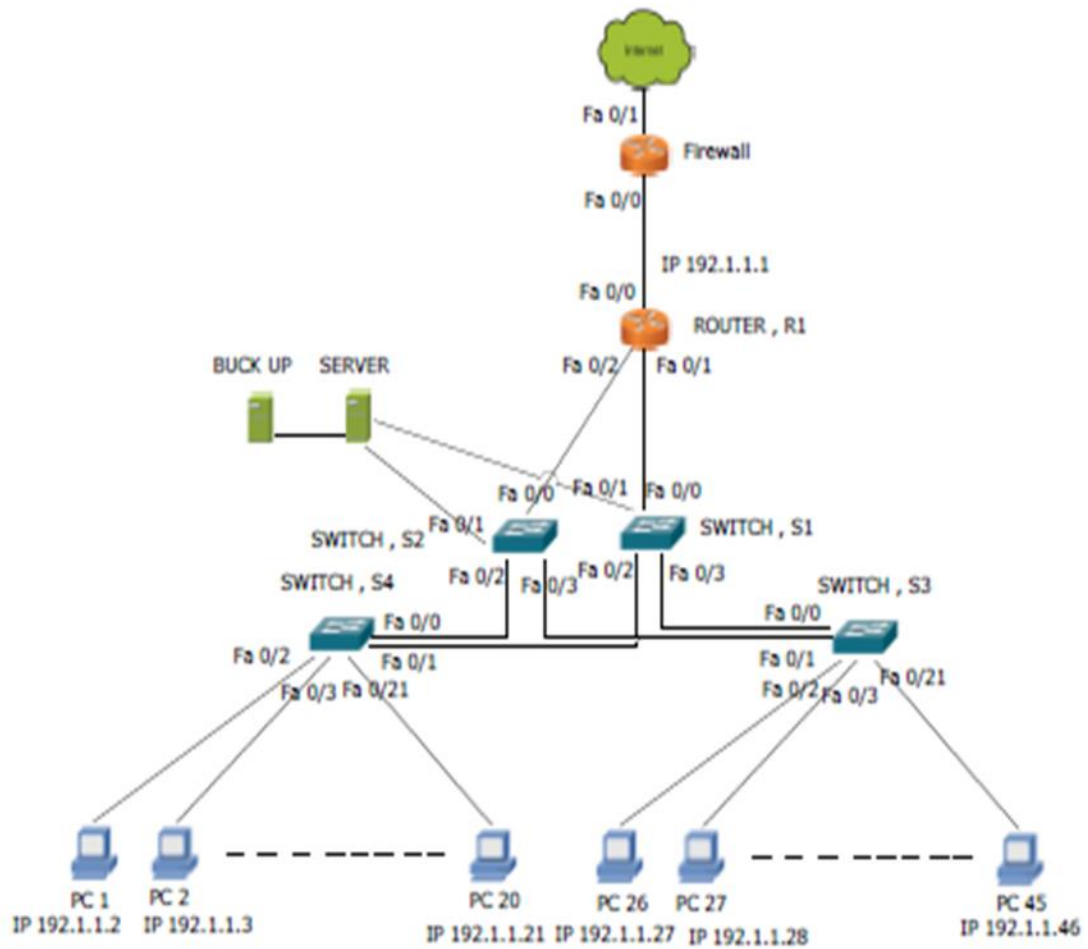


Figure 35 designed mode

5.3 Configuration of switch 1

To starting a switch for the first time, there are three main operations:

- 1- Checks the hardware (Switch).
- 2- Startup the operating system.
- 3- Setting the software configuration.

- **Startup Switch 1**

Switch >enable

Switch # configure terminal

- **Configuring a Host Name**

To give the switch a host name or identify it, use the command, as follows:

Switch (config) # hostname SWITCH, 1S

SWITCH, S1 (config) #

- **Switch Security Understanding**

Security a network by sing some basic suggestions device:

Using a complex password for the devices.

- Using access lists and Limit Telnet access.
- Instead of Telnet we must Use SSE.
- Switch physically secure access.
- For warn against unauthorized access we must use banner
- Doing Configuration for port security.
- Unused ports must be disable.

- **Console password configuring**

SWITCH, 1S > enable

SWITCH, 1S # conf t

SWITCH, 1S (config-if) # line console 0

SWITCH, 1S (config-if) # login

SWITCH, 1S (config-if) # password andazyar

SWITCH, 1S (config-if) # exit

SWITCH, 1S (config-if) # exit

- **Telnet password configuring**

SWITCH, 1S >enable

SWITCH, 1S # conf t

SWITCH, 1S (config-if) # line vty 0 2

SWITCH, 1S (config-if) # login

SWITCH, 1S (config-if) # password andazyar

SWITCH, 1S (config-if) # exit

SWITCH, 1S (config-if) # exit

- **Enable and secret password configuring**

SWITCH, 1S >enable

SWITCH, 1S # conf t

SWITCH, 1S (config-if) # enable password saman

SWITCH, 1S (config-if) # enable secret saman

SWITCH, 1S (config-if) # exit

SWITCH, 1S (config-if) # exit

- **Encrypt password and make it invisible**

SWITCH, 1S >enable

SWITCH, 1S # conf t

SWITCH, 1S (config-if) # service password-encryption

SWITCH, 1S (config-if) # exit

SWITCH, 1S (config-if) # exit

- **Login banner and (MOTD) message of the day configuring**

SWITCH, 1S >enable

SWITCH, 1S # conf t

SWITCH, 1S (config-if) # banner motd \$PLEASE DO NOT ENTER \$

SWITCH, 1S (config-if) # exit

SWITCH, 1S (config-if) # exit

- **SSH Access**

By using SSH to encrypt communication between the SWITCH, 1S and the host. We follow the following steps to configure SSH access:

Step 1. Create a local username and password on the device.

Step 2. Assign a domain name to the device.

Step 3. Generate a security key.

Step 4. Enable SSH.

Step 5. Configure vty ports to authenticate using SSH.

- **Configuring SSH Access**

SWITCH, 1S >enable

SWITCH, 1S # conf t

SWITCH, 1S (config) # user name SAMAN password andazyar

SWITCH, 1S (config) # ip domain-name SAMAN ANDAZYAR

SWITCH, 1S (config) # crypto key generate rsa

SWITCH, 1S (config-if) # no shutdown

SWITCH, 1S (config) # ip ssh version 2

SWITCH, 1S (config) # line vty 0 2

SWITCH, 1S (config) # login local

SWITCH, 1S (config) # transport input ssh

SWITCH, 1S (config-if) # exit

SWITCH, 1S (config-if) # exit

- **Configuring port security**

SWITCH, 1S >enable

SWITCH, 1S # conf t

SWITCH, 1S (config) # interface fa0/0

SWITCH, 1S (config-if) # switchport mod access

SWITCH, 1S (config-if) # switchport port-security

SWITCH, 1S (config-if) # switchport port-security maximum 1

SWITCH, 1S (config-if) # switchport port-security mac-address sticky

SWITCH, 1S (config-if) # switchport port-security violation shutdown

SWITCH, 1S (config) # interface fa0/1

SWITCH, 1S (config-if) # switchport mod access

SWITCH, 1S (config-if) # switchport port-security

SWITCH, 1S (config-if) # switchport port-security maximum 1

SWITCH, 1S (config-if) # switchport port-security mac-address sticky

SWITCH, 1S (config-if) # switchport port-security violation shutdown

SWITCH, 1S (config) # interface fa0/2

SWITCH, 1S (config-if) # switchport mod access

SWITCH, 1S (config-if) # switchport port-security

SWITCH, 1S (config-if) # switchport port-security maximum 1

SWITCH, 1S (config-if) # switchport port-security mac-address sticky

SWITCH, 1S (config-if) # switchport port-security violation shutdown

SWITCH, 1S (config) # interface fa0/3

SWITCH, 1S (config-if) # switchport mod access

SWITCH, 1S (config-if) # switchport port-security

SWITCH, 1S (config-if) # switchport port-security maximum 1

SWITCH, 1S (config-if) # switchport port-security mac-address sticky

SWITCH, 1S (config-if) # switchport port-security violation shutdown

SWITCH, 1S (config-if) # exit

SWITCH, 1S (config-if) # exit

We can secure all unused ports by issuing the shutdown interface command.

5.4 Configuration of switch 2

- **Startup Switch 2**

Switch >enable

Switch # conf t

- **Configuring a Host Name**

To give the switch a host name or identify it, use the command, as follow:

Switch (config) # hostname SWITCH, 2S

- **Console password configuring**

SWITCH, 2S >enable

SWITCH, 2S # conf t

SWITCH, 2S (config-if) # line console 0

SWITCH, 2S (config-if) # login

SWITCH, 2S (config-if) # password andazyar2

SWITCH, 2S (config-if) # exit

SWITCH, 2S (config-if) # exit

- **Telnet password configuring**

SWITCH, 2S >enable

SWITCH, 2S # conf t

SWITCH, 2S (config-if) # line vty 0 2

SWITCH, 2S (config-if) # login

SWITCH, 2S (config-if) # password andazyar2

SWITCH, 2S (config-if) # exit

SWITCH, 2S (config-if) # exit

- **Enable and secret password configuring**

SWITCH, 2S >enable

SWITCH, 2S # conf t

SWITCH, 2S (config-if) # enable password saman2

SWITCH, 2S (config-if) # enable secret saman2

SWITCH, 2S (config-if) # exit

SWITCH, 2S (config-if) # exit

- **To encrypt password and make it invisible**

SWITCH, 2S >enable

SWITCH, 2S # conf t

SWITCH, 2S (config-if) # service password-encryption

SWITCH, 2S (config-if) # exit

SWITCH, 2S (config-if) # exit

- **Login banner and (MOTD) message of the day configuring**

SWITCH, 2S >enable

SWITCH, 2S # conf t

SWITCH, 2S (config-if) # banner motd \$PLEASE DO NOT ENTER \$

SWITCH, 2S (config-if) # exit

SWITCH, 2S (config-if) # exit

- **Configuring SSH Access**

SWITCH, 2S >enable

SWITCH, 2S # configure terminal

SWITCH, 2S (config) # user name SAMAN password andazyar2

SWITCH, 2S (config) # ip domain-name SAMAN ANDAZYAR

SWITCH, 2S (config) # crypto key generate rsa

SWITCH, 2S (config-if) #no shutdown

SWITCH, 2S (config) # ip ssh version 2

SWITCH, 2S (config) # line vty 0 2

SWITCH, 2S (config) # login local

SWITCH, 2S (config) # transport input ssh

SWITCH, 2S (config-if) # exit

SWITCH, 2S (config-if) # exit

- **Configuring port security**

SWITCH, 2S >enable

SWITCH, 2S # configure terminal

SWITCH, 2S (config) # interface fa0/0

SWITCH, 2S (config-if) # switchport mod access

SWITCH, 2S (config-if) # switchport port-security

SWITCH, 2S (config-if) # switchport port-security maximum 1

SWITCH, 2S (config-if) # switchport port-security mac-address sticky

SWITCH, 2S (config-if) # switchport port-security violation shutdown

SWITCH, 2S (config) # interface fa0/1

SWITCH, 2S (config-if) # switchport mod access

SWITCH, 2S (config-if) # switchport port-security

SWITCH, 2S (config-if) # switchport port-security maximum 1

SWITCH, 2S (config-if) # switchport port-security mac-address sticky

SWITCH, 2S (config-if) # switchport port-security violation shutdown

SWITCH, 2S (config) # interface fa0/2

SWITCH, 2S (config-if) # switchport mod access

SWITCH, 2S (config-if) # switchport port-security

SWITCH, 2S (config-if) # switchport port-security maximum 1

SWITCH, 2S (config-if) # switchport port-security mac-address sticky

SWITCH, 2S (config-if) # switchport port-security violation shutdown

SWITCH, 2S (config) # interface fa0/3

SWITCH, 2S (config-if) # switchport mod access

SWITCH, 2S (config-if) # switchport port-security

SWITCH, 2S (config-if) # switchport port-security maximum 1

SWITCH, 2S (config-if) # switchport port-security mac-address sticky

SWITCH, 2S (config-if) # switchport port-security violation shutdown

SWITCH, 2S (config-if) # exit

SWITCH, 2S (config-if) # exit

We secure all unused ports by issuing the shutdown interface command

5.5 Configuration of switch 3

Startup Switch 3

Switch >enable

Switch # conf t

- **Configuring a Host Name**

To give the switch a host name or identify it, use the command, as follow:

Switch (config) # hostname SWITCH, 3S

- **Console password configuring**

SWITCH, 3S >enable

SWITCH, 3S # conf t

SWITCH, 3S (config-if) # line console 0

SWITCH, 3S (config-if) # login

SWITCH, 3S (config-if) # password andazyar3

SWITCH, 3S (config-if) # exit

SWITCH, 3S (config-if) # exit

- **Telnet password configuring**

SWITCH, 3S >enable

SWITCH, 3S # configure terminal

SWITCH, 3S (config-if) # line vty 0 4

SWITCH, 3S (config-if) # login

SWITCH, 3S (config-if) # password andazyar3

SWITCH, 3S (config-if) # exit

SWITCH, 3S (config-if) # exit

- **Enable and secret password configuring**

SWITCH, 3S >enable

SWITCH, 3S # configure terminal

SWITCH, 3S (config-if) # enable password saman3

SWITCH, 3S (config-if) # enable secret saman3

SWITCH, 3S (config-if) # exit

SWITCH, 3S (config-if) # exit

- **To encrypt password and make it invisible**

SWITCH, 3S >enable

SWITCH, 3S # conf t

SWITCH, 3S (config-if) # service password-encryption

SWITCH, 3S (config-if) # exit

SWITCH, 3S (config-if) # exit

- **Login banner and (MOTD) message of the day configuring**

SWITCH, 3S >enable

SWITCH, 3S # configure terminal

SWITCH, 3S (config-if) # banner motd \$PLEASE DO NOT ENTER \$

SWITCH, 3S (config-if) # exit

SWITCH, 3S (config-if) # exit

- **Configuring SSH Access**

SWITCH, 3S >enable

SWITCH, 3S # configure terminal

SWITCH, 3S (config) # user name SAMAN password andazyar3

SWITCH, 3S (config) # ip domain-name SAMAN ANDAZYAR

SWITCH, 3S (config) # crypto key generate rsa

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # ip ssh version 2

SWITCH, 3S (config) # line vty 0 2

SWITCH, 3S (config) # login local

SWITCH, 3S (config) # transport input ssh

SWITCH, 3S (config-if) # exit

SWITCH, 3S (config-if) # exit

- Adding and assigning VLANs to SWITCH, 3S

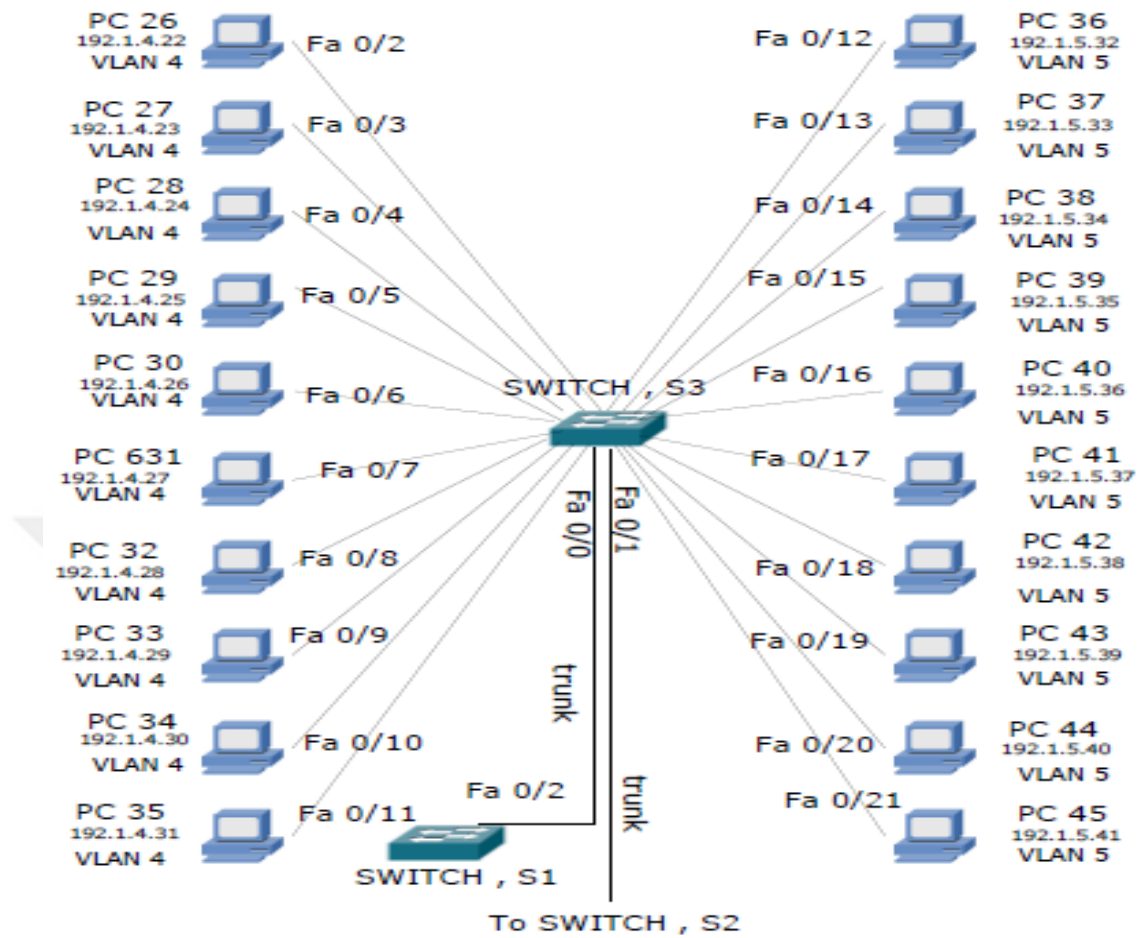


Figure 36 VLAN 4, 5 on SWITCH, 3

SWITCH, 3S >enable

SWITCH, 3S # configure terminal

SWITCH, 3S (config) # vlan 1

SWITCH, 3S (config-vlan) # name ENGINEER

SWITCH, 3S (config) # vlan 2

SWITCH, 3S (config-vlan) # name BOS

SWITCH, 3S (config) # vlan 3

SWITCH, 3S (config-vlan) # name ACCOUNT

SWITCH, 3S (config) # vlan 4

SWITCH, 3S (config-vlan) # name PARTS

SWITCH, 3S (config) # vlan 5

SWITCH, 3S (config-vlan) # name DOCTORS

SWITCH, 3S (config) # interface fa 0/0

SWITCH, 3S (config-if) # switchport mode trunk

SWITCH, 3S (config-if) # switchport trunk native vlan 10

SWITCH, 3S (config-if) # ip address 190.1.100.1 255.255.255.0

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/1

SWITCH, 3S (config-if) # switchport mode trunk

SWITCH, 3S (config-if) # switchport trunk native vlan 10

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/2

SWITCH, 3S (config-if) # switchport mode access

SWITCH, 3S (config-if) # switchport access vlan 4

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/3

SWITCH, 3S (config-if) # switchport mode access

SWITCH, 3S (config-if) # switchport access vlan 4

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/4

SWITCH, 3S (config-if) # switchport mode access

SWITCH, 3S (config-if) # switchport access vlan 4

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/5

SWITCH, 3S (config-if) # switchport mode access

SWITCH, 3S (config-if) # switchport access vlan 4

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/6

SWITCH, 3S (config-if) # switchport mode access

SWITCH, 3S (config-if) # switchport access vlan 4

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/7

SWITCH, 3S (config-if) # switchport mode access

SWITCH, 3S (config-if) # switchport access vlan 4

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/8

SWITCH, 3S (config-if) # switchport mode access

SWITCH, 3S (config-if) # switchport access vlan 4

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/9

SWITCH, 3S (config-if) # switchport mode access

SWITCH, 3S (config-if) # switchport access vlan 4

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/10

SWITCH, 3S (config-if) # switchport mode access

SWITCH, 3S (config-if) # switchport access vlan 4

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/11

SWITCH, 3S (config-if) # switchport mode access

SWITCH, 3S (config-if) # switchport access vlan 4

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/12

SWITCH, 3S (config-if) # switchport mode access

SWITCH, 3S (config-if) # switchport access vlan 5

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/13

SWITCH, 3S (config-if) # switchport mode access

SWITCH, 3S (config-if) # switchport access vlan 5

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/14

SWITCH, 3S (config-if) # switchport mode access

SWITCH, 3S (config-if) # switchport access vlan 5

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/15

SWITCH, 3S (config-if) # switchport mode access

SWITCH, 3S (config-if) # switchport access vlan 5

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/16

SWITCH, 3S (config-if) # switchport mode access

SWITCH, 3S (config-if) # switchport access vlan 5

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/127

SWITCH, 3S (config-if) # switchport mode access

SWITCH, 3S (config-if) # switchport access vlan 5

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/18

SWITCH, 3S (config-if) # switchport mode access

SWITCH, 3S (config-if) # switchport access vlan 5

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/19

SWITCH, 3S (config-if) # switchport mode access

SWITCH, 3S (config-if) # switchport access vlan 5

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/20

SWITCH, 3S (config-if) # switchport mode access

SWITCH, 3S (config-if) # switchport access vlan 5

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config) # interface fa 0/21

SWITCH, 3S (config-if) # switchport mode access

SWITCH, 3S (config-if) # switchport access vlan 5

SWITCH, 3S (config-if) # no shutdown

SWITCH, 3S (config-if) # exit

SWITCH, 3S (config-if) # exit

5.6 Configuration of switch 4

Startup Switch 4

Switch >enable

Switch # conf t

- **Configuring a Host Name**

Switch >enable

Switch # configure terminal

Switch (config) # hostname SWITCH, 4S

SWITCH, 4S (config-if) # exit

SWITCH, 4S (config-if) # exit

- **Console password configuring**

SWITCH, 4S >enable

SWITCH, 4S # configure terminal

SWITCH, 4S (config-if) # line console 0

SWITCH, 4S (config-if) # login

SWITCH, 4S (config-if) # password andazyar4

SWITCH, 4S (config-if) # exit

SWITCH, 4S (config-if) # exit

- **Telnet password configuring**

SWITCH, 4S >enable

SWITCH, 4S # configure terminal

SWITCH, 4S (config-if) # line vty 0 4

SWITCH, 4S (config-if) # login

SWITCH, 4S (config-if) # password andazyar4

SWITCH, 4S (config-if) # exit

SWITCH, 4S (config-if) # exit

- **Enable and secret password configuring**

SWITCH, 4S >enable

SWITCH, 4S # configure terminal

SWITCH, 4S (config-if) # enable password saman4

SWITCH, 4S (config-if) # enable secret saman4

SWITCH, 4S (config-if) # exit

SWITCH, 4S (config-if) # exit

- **To encrypt password and make it invisible**

SWITCH, 4S >enable

SWITCH, 4S # configure terminal

SWITCH, 4S (config-if) # service password-encryption

SWITCH, 4S (config-if) # exit

SWITCH, 4S (config-if) # exit

- **Login banner and (MOTD) message of the day configuring**

SWITCH, 4S >enable

SWITCH, 4S # configure terminal

SWITCH, 4S (config-if) # banner motd \$PLEASE DO NOT ENTER \$

SWITCH, 3S (config-if) # exit

SWITCH, 4S (config-if) # exit

- **Configuring SSH Access**

SWITCH, 4S >enable

SWITCH, 4S # configure terminal

SWITCH, 4S (config) # user name SAMAN password andazyar3

SWITCH, 4S (config) # ip domain-name SAMAN ANDAZYAR

SWITCH, 4S (config) # crypto key generate rsa.

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # ip ssh version 2

SWITCH, 4S (config) # line vty 0 2

SWITCH, 4S (config) # login local

SWITCH, 4S (config) # transport input ssh

SWITCH, 4S (config-if) # exit

SWITCH, 4S (config-if) # exit

- Adding and assigning VLANs to SWITCH, S4

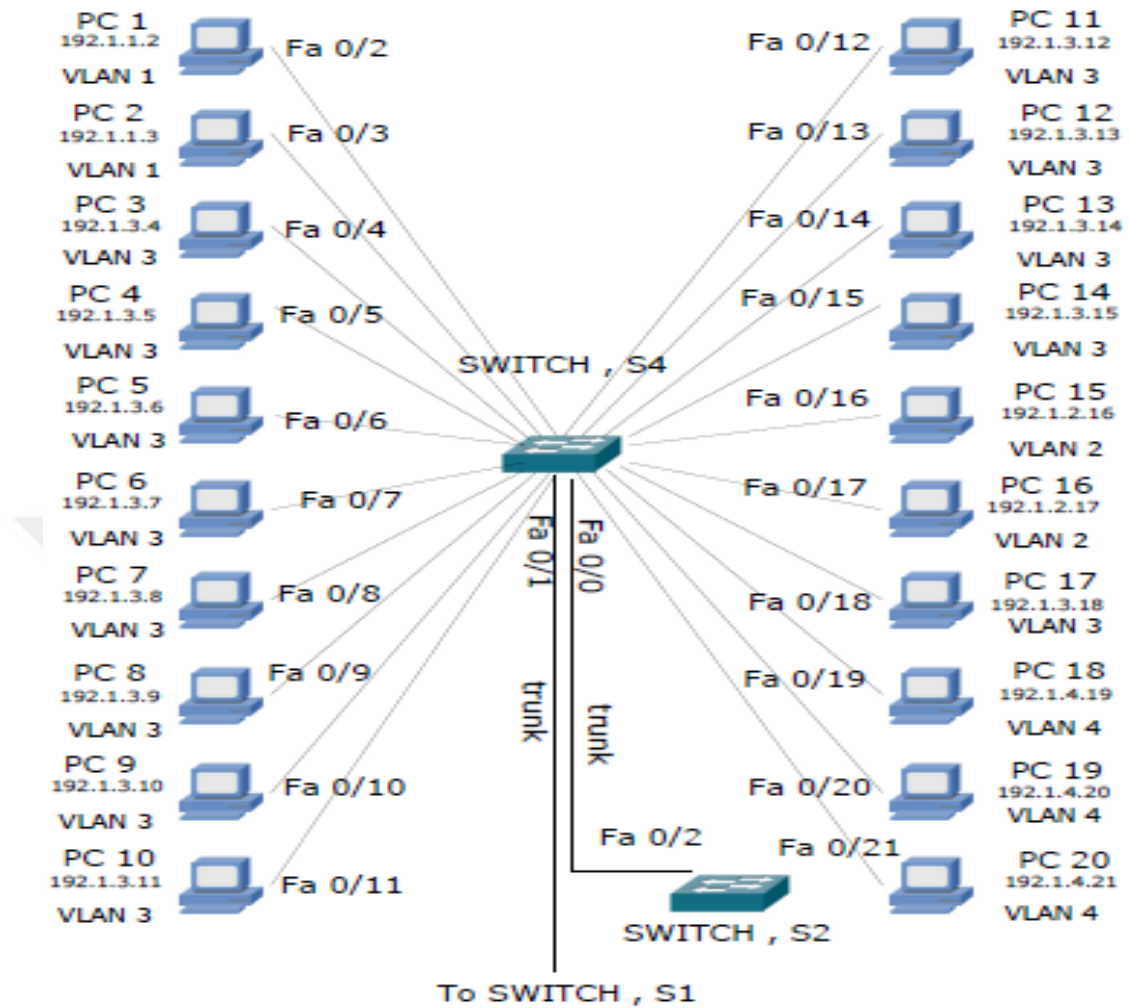


Figure 37 VLAN 1, 2, 3, 4 on SWITCH, 4

SWITCH, 4S >enable

SWITCH, 4S # configure terminal

SWITCH, 4S (config) # vlan 1

SWITCH, 4S (config-vlan) # name ENGINEER

SWITCH, 4S (config) # vlan 2

SWITCH, 4S (config-vlan) # name BOS

SWITCH, 4S (config) # vlan 3

SWITCH, 4S (config-vlan) # name ACCOUNT

SWITCH, 4S (config) # vlan 4

SWITCH, 4S (config-vlan) # name PARTS

SWITCH, 4S (config) # vlan 5

SWITCH, 4S (config-vlan) # name DOCTORS

SWITCH, 4S (config) # interface fa 0/0

SWITCH, 4S (config-if) # switchport mode trunk

SWITCH, 4S (config-if) # switchport trunk native vlan 10

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/1

SWITCH, 4S (config-if) # switchport mode trunk

SWITCH, 4S (config-if) # switchport trunk native vlan 10

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/2

SWITCH, 4S (config-if) # switchport mode access

SWITCH, 4S (config-if) # switchport access vlan 1

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/3

SWITCH, 4S (config-if) # switchport mode access

SWITCH, 4S (config-if) # switchport access vlan 1

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/4

SWITCH, 4S (config-if) # switchport mode access

SWITCH, 4S (config-if) # switchport access vlan 3

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/5

SWITCH, 4S (config-if) # switchport mode access

SWITCH, 4S (config-if) # switchport access vlan 3

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/6

SWITCH, 4S (config-if) # switchport mode access

SWITCH, 4S (config-if) # switchport access vlan 3

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/7

SWITCH, 4S (config-if) # switchport mode access

SWITCH, 4S (config-if) # switchport access vlan 3

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/8

SWITCH, 4S (config-if) # switchport mode access

SWITCH, 4S (config-if) # switchport access vlan 3

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/9

SWITCH, 4S (config-if) # switchport mode access

SWITCH, 4S4 (config-if) # switchport access vlan 3

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/10

SWITCH, 4S (config-if) # switchport mode access

SWITCH, 4S (config-if) # switchport access vlan 3

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/11

SWITCH, 4S (config-if) # switchport mode access

SWITCH, 4S (config-if) # switchport access vlan 3

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/12

SWITCH, 4S (config-if) # switchport mode access

SWITCH, 4S (config-if) # switchport access vlan 3

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/13

SWITCH, 4S (config-if) # switchport mode access

SWITCH, 4S (config-if) # switchport access vlan 3

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/14

SWITCH, 4S (config-if) # switchport mode access

SWITCH, 4S (config-if) # switchport access vlan 3

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/15

SWITCH, 4S (config-if) # switchport mode access

SWITCH, 4S (config-if) # switchport access vlan 3

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/18

SWITCH, 4S (config-if) # switchport mode access

SWITCH, 4S (config-if) # switchport access vlan 3

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/16

SWITCH, 4S (config-if) # switchport mode access

SWITCH, 4S (config-if) # switchport access vlan 2

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/17

SWITCH, 4S (config-if) # switchport mode access

SWITCH, 4S (config-if) # switchport access vlan 2

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/19

```
SWITCH, 4S (config-if) # switchport mode access

SWITCH, 4S (config-if) # switchport access vlan 4

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/20

SWITCH, 4S (config-if) # switchport mode access

SWITCH, 4S (config-if) # switchport access vlan 4

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config) # interface fa 0/21

SWITCH, 4S (config-if) # switchport mode access

SWITCH, 4S (config-if) # switchport access vlan 4

SWITCH, 4S (config-if) # no shutdown

SWITCH, 4S (config-if) # exit

SWITCH, 4S (config-if) # exit
```

5.7 Configuration of Router 1

From the mode of EXEC. We can access these specific configuration modes, with the global mode configuration:

- Interface configuration.
- Sub interface configuration.
- Controlled configuration.
- Line configuration.
- Route configuration.

- **Startup Router 1**

Router >enable

Route # conf t

- **Configuring a Host Name**

To give the Router a host name or identify it, use the command, as follow:

Router >enable

Route # configure terminal

Router (config) # hostname ROUTER, R1

ROUTER, R1# exit

ROUTER, R1# exit

- **Console password configuring**

ROUTER, R1>enable

ROUTER, R1# configure terminal

ROUTER, R1 (config) # line console 0

ROUTER, R1 (config-line) # login

ROUTER, R1 (config-line) # password andazyar5

ROUTER, R1# exit

ROUTER, R1# exit

- **Configuring (NAT) network address translation and the Router interface IP Address (static).**

ROUTER, R1>enable

ROUTER, R1# configure terminal

ROUTER, R1 (config) # interface fa0/0

ROUTER, R1 (config-if) # ip add 192.1.1.1 255.255.255.0

ROUTER, R1 (config-if) # no shutdown

ROUTER, R1 (config-if) # ip nat inside

ROUTER, R1 (config) # interface fa0/1

ROUTER, R1 (config-if) # ip add 6.1.1.1 255.0.0.0

ROUTER, R1 (config-if) # no shutdown

ROUTER, R1 (config-if) # ip nat outside

ROUTER, R1 (config-if) #exit

ROUTER, R1 (config) # nat inside source static 192.1.1.2 5.1.1.2

ROUTER, R1 (config) # nat inside source static 192.1.1.3 5.1.1.3

ROUTER, R1 (config) # nat inside source static 192.1.1.4 5.1.1.4

ROUTER, R1 (config) # nat inside source static 192.1.1.5 5.1.1.5

ROUTER, R1 (config) # nat inside source static 192.1.1.6 5.1.1.6

ROUTER, R1 (config) # nat inside source static 192.1.1.7 5.1.1.7

ROUTER, R1 (config) # nat inside source static 192.1.1.8 5.1.1.8

ROUTER, R1 (config) # nat inside source static 192.1.1.9 5.1.1.9

ROUTER, R1 (config) # nat inside source static 192.1.1.10 5.1.1.10

ROUTER, R1 (config) # nat inside source static 192.1.1.11 5.1.1.11

ROUTER, R1 (config) # nat inside source static 192.1.1.12 5.1.1.12

ROUTER, R1 (config) # nat inside source static 192.1.1.13 5.1.1.13

ROUTER, R1 (config) # nat inside source static 192.1.1.14 5.1.1.14

ROUTER, R1 (config) # nat inside source static 192.1.1.15 5.1.1.15

ROUTER, R1 (config) # nat inside source static 192.1.1.16 5.1.1.16

ROUTER, R1 (config) # nat inside source static 192.1.1.17 5.1.1.17

ROUTER, R1 (config) # nat inside source static 192.1.1.18 5.1.1.18

ROUTER, R1 (config) # nat inside source static 192.1.1.19 5.1.1.19

ROUTER, R1 (config) # nat inside source static 192.1.1.20 5.1.1.20

ROUTER, R1 (config) # nat inside source static 192.1.1.26 5.1.1.26

ROUTER, R1 (config) # nat inside source static 192.1.1. 27 5.1.1.27

ROUTER, R1 (config) # nat inside source static 192.1.1.28 5.1.1.28

ROUTER, R1 (config) # nat inside source static 192.1.1.29 5.1.1.29

ROUTER, R1 (config) # nat inside source static 192.1.1.30 5.1.1.30

ROUTER, R1 (config) # nat inside source static 192.1.1.31 5.1.1.31

ROUTER, R1 (config) # nat inside source static 192.1.1.32 5.1.1.32

ROUTER, R1 (config) # nat inside source static 192.1.1.33 5.1.1.33

ROUTER, R1 (config) # nat inside source static 192.1.1.34 5.1.1.34

ROUTER, R1 (config) # nat inside source static 192.1.1.35 5.1.1.35

ROUTER, R1 (config) # nat inside source static 192.1.1.36 5.1.1.36

ROUTER, R1 (config) # nat inside source static 192.1.1.37 5.1.1.37

ROUTER, R1 (config) # nat inside source static 192.1.1.38 5.1.1.38

ROUTER, R1 (config) # nat inside source static 192.1.1.39 5.1.1.39

ROUTER, R1 (config) # nat inside source static 192.1.1.40 5.1.1.40

ROUTER, R1 (config) # nat inside source static 192.1.1.41 5.1.1.41

ROUTER, R1 (config) # nat inside source static 192.1.1.42 5.1.1.42

ROUTER, R1 (config) # nat inside source static 192.1.1.43 5.1.1.43

ROUTER, R1 (config) # nat inside source static 192.1.1.44 5.1.1.44

ROUTER, R1 (config) # nat inside source static 192.1.1.45 5.1.1.45

ROUTER, R1# exit

ROUTER, R1# exit

- **Configuring (NAT) network address translation and the Router interface IP Address (dynamic).**

ROUTER, R1>enable

ROUTER, R1# configure terminal

ROUTER, R1 (config) # interface fa0/0

ROUTER, R1 (config-if) # ip add 192.1.1.1 255.255.255.0

ROUTER, R1 (config-if) # no shutdown

ROUTER, R1 (config-if) # ip nat inside

ROUTER, R1 (config) # interface fa0/1

ROUTER, R1 (config-if) # ip add 6.1.1.1 255.0.0.0

ROUTER, R1 (config-if) # no shutdown

ROUTER, R1 (config-if) # ip nat outside

ROUTER, R1 (config-if) #exit

ROUTER, R1 (config) # ip nat pool FLOOR 1 6.1.1.1 6.1.1.200 natmask 255.0.0.0

ROUTER, R1 (config) # access-list 50 permit 192.1.1.0 0.0.0.255

ROUTER, R1 (config) # nat inside source-list 50 pool FLOOR 1

ROUTER, R1# exit

ROUTER, R1# exit

- **(PAT) NAT overload Configuring**

ROUTER, R1>enable

ROUTER, R1# configure terminal

ROUTER, R1 (config) # interface fa0/0

ROUTER, R1 (config-if) # ip add 192.1.1.1 255.255.255.0

ROUTER, R1 (config-if) # no shutdown

ROUTER, R1 (config-if) # ip nat inside

ROUTER, R1 (config) # interface fa0/1

ROUTER, R1 (config-if) # ip add 6.1.1.1 255.0.0.0

ROUTER, R1 (config-if) # no shutdown

ROUTER, R1 (config-if) # ip nat outside

ROUTER, R1 (config-if) #exit

ROUTER, R1 (config) # nat pool FLOOR 1 6.1.1.1 6.1.1.200 natmask 255.0.0.0

ROUTER, R1 (config) # access-list 50 permit 192.1.1.0 0.0.0.255

ROUTER, R1 (config) # nat inside source-list 50 pool FLOOR 1 overload

ROUTER, R1# exit

ROUTER, R1# exit

- **Telnet password configuring**

ROUTER, R1>enable

ROUTER, R1# configure terminal

ROUTER, R1 (config-if) # line vty 0 2

ROUTER, R1 (config-if) # login

ROUTER, R1 (config-if) # password andazyar3

ROUTER, R1 (config) # nat inside source list 50 permit

ROUTER, R1# exit

ROUTER, R1# exit

- **Enable and secret password configuring**

ROUTER, R1>enable

ROUTER, R1# configure terminal

ROUTER, R1 (config-if) # enable password saman3

ROUTER, R1 (config-if) # enable secret saman3

ROUTER, R1# exit

ROUTER, R1# exit

- **To encrypt password and make it invisible**

ROUTER, R1 (config-if) # service password-encryption

- **Login banner and (MOTD) message of the day configuring**

ROUTER, R1>enable

ROUTER, R1# configure terminal

ROUTER, R1 (config-if) # banner motd \$PLEASE DO NOT ENTER \$

ROUTER, R1# exit

ROUTER, R1# exit

- **Configuring SSH Access**

ROUTER, R1>enable

ROUTER, R1# configure terminal

ROUTER, R1 (config) # user name SAMAN password andazyar3

ROUTER, R1 (config) # ip domain-name SAMAN ANDAZYAR

ROUTER, R1 (config) # crypto key generate rsa

ROUTER, R1 (config-if) # no shutdown

ROUTER, R1 (config) # ip ssh version 2

ROUTER, R1 (config) # line vty 0 2

ROUTER, R1 (config) # login local

ROUTER, R1 (config) # transport input ssh

ROUTER, R1# exit

ROUTER, R1# exit

- **Net flow analysis**

ROUTER, R1>enable

ROUTER, R1# configure terminal

ROUTER, R1 (config) # int fa0/0

ROUTER, R1 (config-if) # ip router-cache flow

ROUTER, R1 (config-if) # ip flow-export source fa0/0

ROUTER, R1 (config-if) # ip flow-export destination 6.1.1.2 2055

ROUTER, R1 (config-if) # ip flow-export version 5

ROUTER, R1 (config-if) # ip flow-export timeout active 5

ROUTER, R1 (config-if) # ip slow-cache timeout inactive 15

ROUTER, R1# exit

ROUTER, R1# exit

- **Configuring Extended IP access lists**

ROUTER, R1>enable

ROUTER, R1# conf t

ROUTER, R1 (config-if) # int fa0/0

ROUTER, R1 (config-if) # ip access-list extended BLOCKING WWW

ROUTER, R1 (config-if) # deny tcp host 190.1.1.1

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.3.4

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.3.5

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.3.6

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.3.7

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.3.8

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.3.9

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.3.10

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.3.11

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.3.12

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.3.13

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.3.4

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.3.15

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.3.18

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.4.19

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.4.20

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.4.21

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.4.22

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.4.23

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.4.24

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.4.25

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.4.26

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.4.27

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.4.28

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.4.29

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.4.30

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.4.31

ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.5.32

```
ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.5.33
ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.5.34
ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.5.35
ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.5.36
ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.5.37
ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.5.38
ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.5.39
ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.5.40
ROUTER, R1 (config-if) # ip access-list 1 deny host 192.1.5.41
ROUTER, R1 (config-if) # ip permit any any
ROUTER, R1# exit
ROUTER, R1# exit
```

5.8 Configure PC to local area network

Configuration PC to the LAN to connect to the network and internet, then look no further. Here are steps and guidelines on how to configure your PC to a local area network [41, 42, 43].

- 1- By using a cable contact with RJ-45 from your PC.
- 2- Click On 'PC '.
- 3- Select desktop
- 4- Click on 'IP configuration'.
- 5- Click 'OK'.

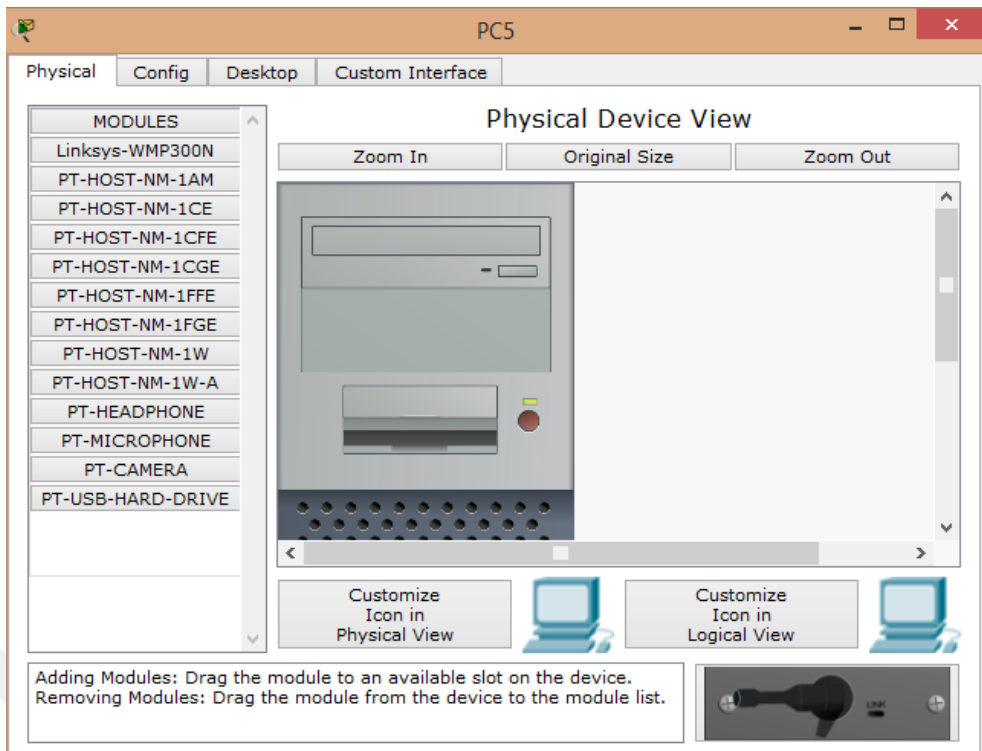


Figure 38 Config. The PC to (LAN) step 1

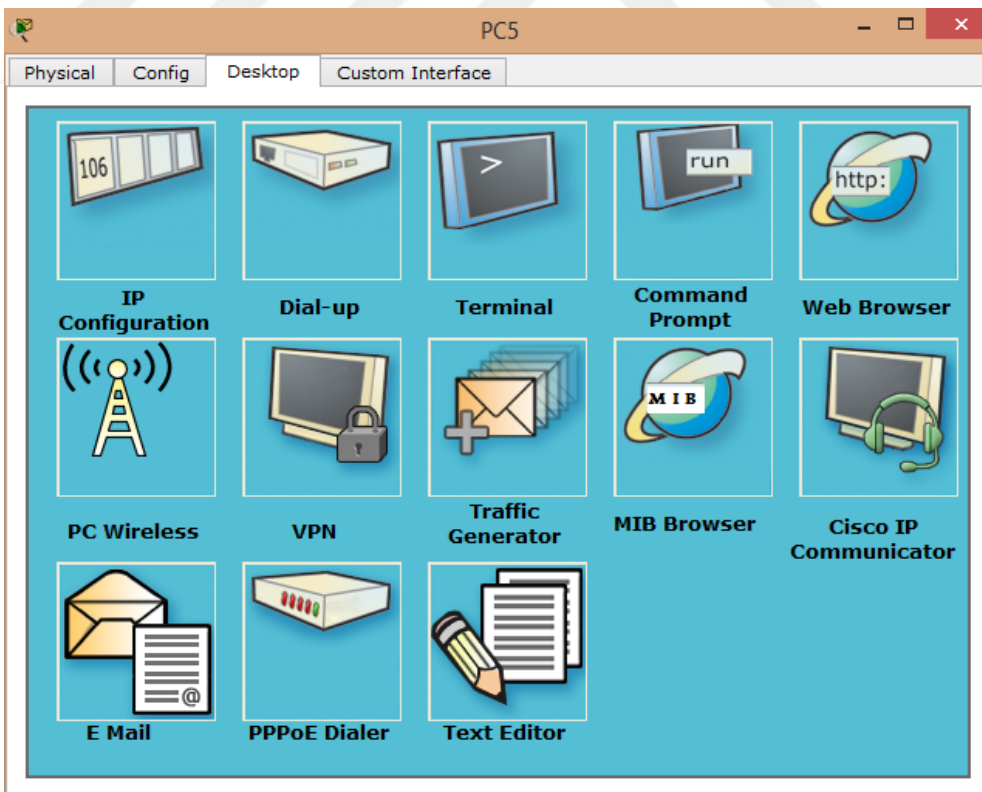


Figure 39 Config.the PC to (LAN) step 2

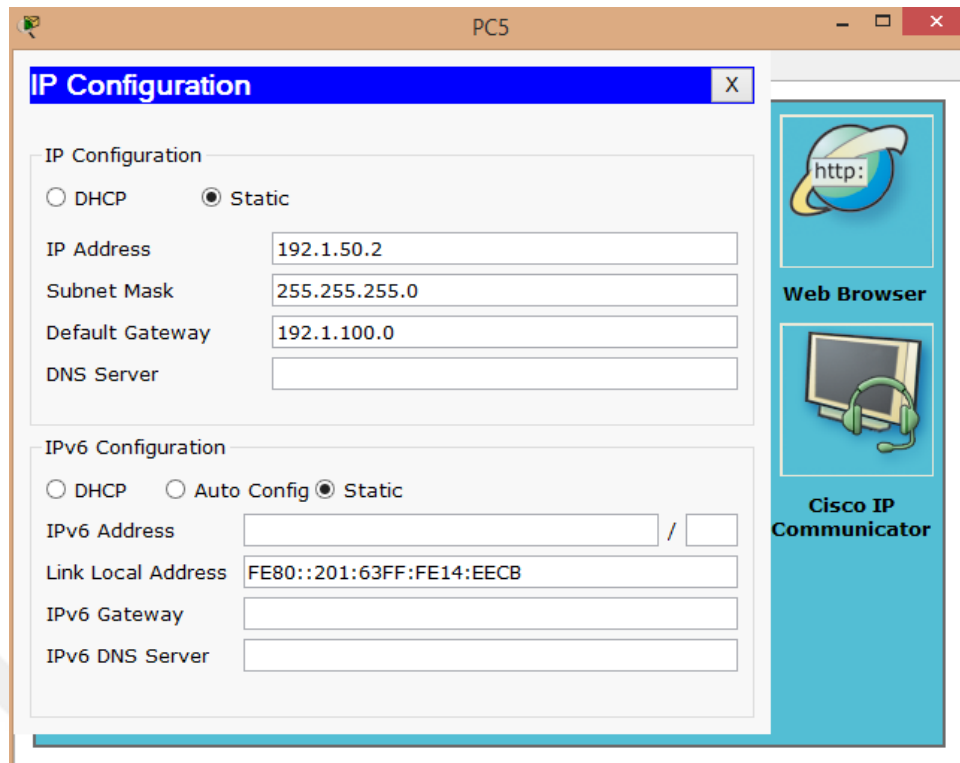


Figure 40 Config.the PC to (LAN) step 3

5.9 Configure Firewall

This is simply turning the firewall on/off. If you've installed Windows, chances are the operating system has already set up your router while installation. You can set it up manually too, using a browser of your preference [43, 44].

- 1- Type router IP address in a browser
 - 2- Check for Firewall option on the router homepage.
 - 3- A activate the firewall.
- **Disable Router Firewall**

We can run a firewall on both router (hardware firewall) and computer (software firewall) that can prove to be useful as we have multiple lines of defense when it comes to dealing with attacks. However, in rare cases, disabling the firewall on a router can resolve conflicts caused when both the router's firewall and the operating system's firewall are turned on at the same time. Disabling firewalls on either your router or

computer is not encouraged, but it can most certainly be done. Access to the router's web interface will be required in order to disable the router firewall. This article provides detailed instructions on how to disable the firewall on a router from the router's web interface [45].

- **Set up a Router Firewall**

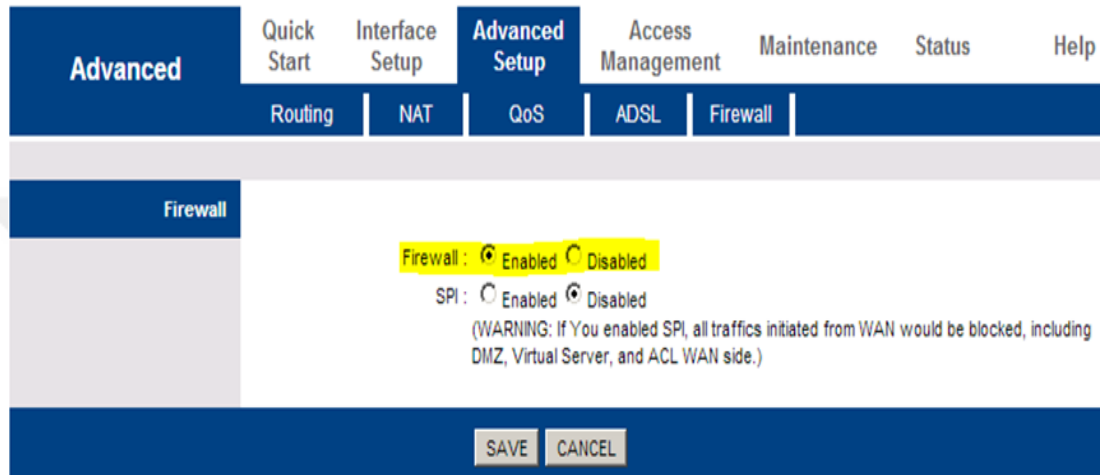


Figure 41 firewall configuration

CHAPTER 6

CONCLUSION AND SUGGESTION FOR FUTURE WORK

6.1 CONCLUSION

In the beginning of the planning on modern hospital buildings stages. The engineers should make planning about the need for a very high level of security and safety, a reducing environment contamination, the merger of renewable for power and reducing costs must be taken into the accounts in order to investment the full possible of economic competencies and investigation technical needed.

The aim with my master thesis was to design a network for management of hospital information system by using a computer network to implementation this hospital information system and using protection against intrusion. It is so important to guaranty that information in saving and transferring should not be get, modification or manipulation by unwanted people may led to big damages. Research on new network design that has a security methods to improvement the security of the network of save a hospital information system (HIS). This is very needed to save the system from deny any attack. Security architecture was optimized but researching are the best means to save the network from attackers.

6.2 Suggestion for future works

- 1- Improvements for implementing a secure WLAN network for hospitals and ministry of health.
- 2- Merge applications of hashing advantages in to the form for the system and using firewall device. This will lead to more security.
- 3- Adding some new rules can be included to further development of the network security and hospital information system on the usefulness of the current prototype

- 4- Using electrical system that consist of all the requirements of a system that includes the better types of the equipment.



REFERENCES

- [1] Yusuf B. (2008). Network Security Technologies and Solutions.
- [2] James J., Morgan K. (2008). Network Security: Know It All.
- [3] Joe H. (2002). Cisco Network Security Little Black Book. Paraglyph Press.
- [4] Kevin D., Ian B. (2006). Cisco IOS Cookbook. O'Reilly Media.
- [5] Andrew S., Tanenbaum. (2003). Computer Networks, Fourth Edition Prentice Hall.
- [6] Wears R. L., Berg M. (2005). Computer Technology and Clinical Work: Still Waiting for Godoy, *Journal of American Medical Association*. 293(10), pp. 1261-1263.
- [7] Kevin H., Kennedy C. (1999). Cisco LAN Switching (CCIE Professional Development).
- [8] Annabel Z.D. (1999). The Essential Guide to Telecommunications, Second Edition Prentice Hall.
- [9] Sergio V. (2000). Wireless bandwidth in the making. IEEE.
- [10] Gene S., Simson G., & Alan S. (2003). Practical Unix & Internet Security, 3rd Edition.
- [11] Fred H., Addison W. (1996). Data Communications, Computer Networks and Open Systems, Fourth Edition.
- [12] William S. (1984). Local networks. ACM.
- [13] Mahbub H., Raj J., & Pearson P. (2004). High Performance TCP/IP Networking.

- [14] Richard S., Addison W. (1993). *The Protocols (TCP/IP Illustrated, Volume 1)*.
- [15] Matt B., Addison W. (2002). *Computer Security, Art and Science*.
- [16] Cross-Industry Working Team. (2000). *Internet service performance: Data analysis and visualization*.
- [17] Kundur, P. (1994). *Power system stability and control (Vol. 7)*.
- [18] Padiyar, K. R. (2007). *FACTS controllers in power transmission and distribution*. New Age International.
- [19] Kundur, P. (1994). *Power system stability and control (Vol. 7)*. N. J. Balu, & M. G. Lauby (Eds.). New York: McGraw-hill.
- [20] Kundur, P., Paserba, J., Ajarapu, V., Andersson, G., Bose, A., Canizares, C., & Vittal, V. (2004). Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions. *Power Systems, IEEE Transactions on*, 19(3), 1387-1401.
- [21] Lee, D.C. (1992). Energy development and power of generation committee of power generation society, IEEE recommended practice for excitation system models for power system stability studies.
- [22] Gmbh D. (2013). *Power system stability on island networks*, Prepared for IRENA Workshop, Palau.
- [23] Mark B. (2004). *Analytical Network and System Administration*.
- [24] Sellitto C. and Carbone D. (2007). Success Factors Associated with Health Information System Implementation: *A Study of an Australian Regional Hospital, Journal of Business Systems, Governance and Ethics, Victoria University, Melbourne, Australia*.
- [25] Sittig, D. F. (2001). The importance of Leadership in the Clinical Information System implementation process. *E-journal of the Association of Medical Directors of Information Systems and the Improve-IT Institute*.

- [26] Winkelman, W.J., Leonard, K.J. (2004). Overcoming Structural Constraints to Patient Utilization of Electronic Medical Records: *A Critical Review and Proposal for an Evaluation Framework*. *Journal of the American Medical Informatics Association*. 11(2), pp. 151-161.
- [27] Berg M. (1999). Patient Care Information Systems and Health Care Work: *A Socio-technical Approach*. *International journal of Medical Informatics*, 55(2), pp. 87-101.
- [28] Malik A. M., Khan R. H. (2009). Understanding the Implementation of an electronic hospital information system in a developing country, a case study from Pakistan, 3rd Australasian Workshop on HIKM, Wellington, New Zealand.
- [29] Wright M. K. & Capps C. J. (2010). Information Systems Development Project Performance in the 21st Century. *Software Engineering Notes*, Vol. 35(2).
- [30] Baus A. (2004). Barriers to the Successful Implementation of Healthcare Information Systems, West Virginia University department of community medicine, Office of Health Services Research.
- [31] Bruce S., Davie L., & Peterson M. (2000). *Computer Networks - A System Approach*, Second Edition.
- [32] Clifford N., Theodore T. (1994). Kerberos: An Authentication Service for Computer Networks. *IEEE Communications Magazines*.
- [33] Nikita B., Ian G., & David W. (2001). Intercepting Mobile Communications: The Insecurity of 802.11. *Proceedings of the 7^o Annual International Conference on Mobile Computing and Networking*.
- [34] Wannous M., & Nakano H. (2010). NVLab, a networking virtual web-based laboratory that implements virtualization and virtual network computing technologies.
- [35] Dainotti A., Squarcella C., Aben E, Claffy K. C., Chiesa M., & Pescapé A. (2011). Analysis of country-wide internet outages caused by censorship. in *Proc. ACM SIGCOMM Conf. Internet Measurement*, New York, NY, USA, pp. 1–18, ACM, ser. IMC'11.

- [36] Wagner P. J., & Wudi J. M. (2004). Designing and implementing a cyberwar laboratory exercise for a computer security course. In Proc. 35th SIGCSE Tech. Symp. Computer Science Education, New York, NY, USA, 2004, pp. 402–406, ACM.
- [37] Finseth C. (1993). An Access Control Protocol, Sometimes Called TACACS.
- [38] Marsa I., Hoz E., Gimenez G., & Lopez C. (2012). Using a scenario-generation framework for education on system and internet security. In Proc. IEEE Global Engineering Education Conf. EDUCON, Marrakesh, Morocco, pp. 1–7.
- [39] Ben Othmane L., Bhuse V., & Lilien L. (2013). Incorporating lab experience into computer security courses, in Proc. World Congr. Computer and Information Technology (WCCIT). IEEE Trans. Learn. Tech., vol. 3, no. 2, pp. 129–138.
- [40] Abler D., Contis J., & Owen H. L. (2006). Georgia Tech information security center hands-on network security laboratory. IEEE Trans. Edu., vol. 49, no. 1, pp. 82–87.
- [41] Lee C., Uluagac A., Fairbanks K., & Copeland J. (2011). The design of net-Security Lab: A small competition-based network security lab. IEEE Trans. Trans. Edu. vol. 54, no. 1, pp. 149–155.
- [42] Adam S., John I., & Avid D. (2001). Using the Fluhrer, Mantin, a Shamir Attack to Break WEP. AT&T Labs Technical Report TD-4ZCPZZ.
- [43] Droms R. (1997). Dynamic Host Configuration Protocol. RFC 2131.
- [44] Joseph D. (2001). Network Troubleshooting Tools. O'Reilly.
- [45] Miroslaw M., Allen M. (1988). Survey of software tools for evaluating reliability, availability, and serviceability. ACM Computing Surveys.