A Mini Project Report on

# AN ENTERPRISE NETWORK OF A HOSPITAL USING CISCO PACKET TRACER

*Submitted in partial fulfillment of the requirements*

*Of The Semester VII subject of*

*Network Design Lab*

*In*

*Information Technology*

*By*

**Zarrar Husain Zakir Husain Khan**

**Roll No.: 29**

**Sanap Ghanshyam Vasantrao**

**Roll No.: 56**

**Mitesh Latish Bauskar**

**Roll No.: 03**

*Under the supervision of*

**Prof. V. M. Kharche**

DEPARTMENT OF INFORMATION TECHNOLOGY

KONKAN GYANPEETH COLLEGE OF ENGINEERING

KARJAT-410201

2020-2021

# Certificate

This is to certify that the Network Design Lab (NDL) Mini Project entitled **An Enterprise Network of A Hospital using Cisco Packet Tracer** is submitted by Zarrar Husain Khan (Roll No.29), Ghanshyam Sanap (Roll No.56), Mitesh Bauskar (Roll No.03) for the partial fulfillment of the requirement for Semester VII Subject of Network Design Lab in BE Information Technology to the University of Mumbai, is a bonafide work carried out during Semester VII in Academic Year 2020-2021

| | |
|---|---|
| Prof. V. M. Kharche | Dr. A. W. Kale |
| **Subject In-Charge** | **Head of Department** |
| Sub: END (NDL) | Department of Information Technology |

**External Examiner(s):**

1…………………………………..

2…………………………………..

**Place:**

**Date:**

# Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

**Signature**

**(Zarrar Husain Khan) Roll No.:29**

**Signature**

**(Ghanshyam Sanap) Roll No.:56**

**Signature**

**(Mitesh Bauskar) Roll No.:03**

**Date:**

# Abstract

The network design is a major part of the infrastructure of a hospital. Internet speed is a major component of ensuring that healthcare providers and other professionals achieve timely access to pertinent information. The main aim of this paper is to design a hospital network which meets the requirements of a hospital network like electronic health records, on-call doctors via video communication, billing department records, keeping track of the research in progress, etc. The aim is to provide secured LAN and WLAN network. The network is designed by keeping in mind of upcoming technology in medical field. This will increase the quality of hospital service along with patient safety and clinical effectiveness.

# Acknowledgement

Before we get into think of the things we would like to add a few heartfelt words for the people who were part of this project and help us in numerous ways. People who gave unending support right from the initial stages of the development of project.

We are thankful to our project coordinator **Prof. V. M. Kharche** for their guidance in selecting our project and providing proper support for performing given tasks of project.

We would extend our sincerest gratitude to our HEAD OF DEPARTMENT as well as our guide **Dr. A. W. Kale** for guiding us throughout the project and making it better than we could have thought. His inexorable direction and profound experience motivated and inspired us. This project would not be possible without their help. Thank you to all our professors and non-teaching staff who were directly or in-directly involved in making the project success.

# Table of Contents

# Introduction:

The field of Information Technology and Network Infrastructure Management has become a crucial component inside the healthcare industry. Medical experts are working along with the IT departments to create more medical devices that can be connected to the network, hence providing doctors the facility to monitor patients easily over internet. Also, hospitals have initiated the method of electronic health records which are easy to access for doctors as well as the patient’s family members. There are several times when a doctor can’t be present and this factor has already been overcome by video communication. The hospital network has to be made secure as well so that essential data like medical records and research work does not fall into the wrong hands.

In general, in designing and maintaining the performance, efficiency, architecture and security of the hospital network, the IT manager faces a lot of challenges. An important consideration of network design for today's networks is creating the potential to reliably, scalably and securely support future expansion.

We need to design a network topology that is easy to understand, easy to manage, easy to troubleshoot and is adaptable to change in future according to the new medical equipment. Among the various topologies like bus topology, ring topology, mesh topology, star topology, etc., Hierarchical topology would best meet our demands. The hierarchical network design model serves to help us develop a network topology in separate layers. Each layer focuses on specific functions, enabling us to choose the right equipment and features for the layer. A hierarchical design avoids the need for a fully meshed network in which all network nodes are interconnected and thus making it simple and easy to understand.

# Objectives:

The main objective of our project:

The primary objective of this research paper is to provide state of the art networking facilities for the IP-based medical devices, doctors, nurses, visitors and working staff of the hospital. Given below the points to throw light on the subject matter:

- Providing remote medical consultancy or to supervise the surgery/operation from remote location.
- Uninterrupted high speed internet connectivity.
- Provide better medical facilities to the patients.
- Organized health records for future use.
- Uninterrupted communication between different departments of the hospital.
- Reducing the workload at nurse station, account department, reception desk.
- Keeping the research work of the doctors and medical records of patients secure.
- Providing limited internet access for the visitors

## Network Requirements:

The proposal is to design a state of the art network for a district level hospital. The hospital consists of various departments separated among three buildings. The distance between two buildings is 50 meters. Each building has four floors. Each building has its own reception desk on the ground floor with two desktops, one central medical store and medical store room having two desktops. Each floor has three wings, and each wing has its own nurse stations containing one desktop. Apart from this there were medical instruments requiring both wired and wireless internet connectivity. Visitors of the hospitals would get limited wireless connectivity.

# Major Design Areas & Functional Areas:

The following are the major design areas to be addressed:

Step 1: Identify the relevant network applications, their logical connectivity requirements, and the services required as part of the initial design.
Step 2: Divide the network into modules.
Step 3: Identify the scope of the design to decide which modules are to be redesigned.
Step 4: Identify design alternatives for each module, including the following:

a. Redesign the Hospital LAN: The current Hospital LAN is shared and interconnects three buildings. Because there is no redundancy, the designer needs to entirely redesign the Shopping, including the placement of servers.

b. Redesign the IP addressing scheme: The flat addressing scheme and static routes are not desirable features in a scalable growing network. New hierarchical addressing is required.

c. Introduce a new routing protocol: The network is aware of the drawbacks of static routes. The designer should implement a dynamic routing protocol that is more scalable and that better fits the planned hierarchical addressing scheme.

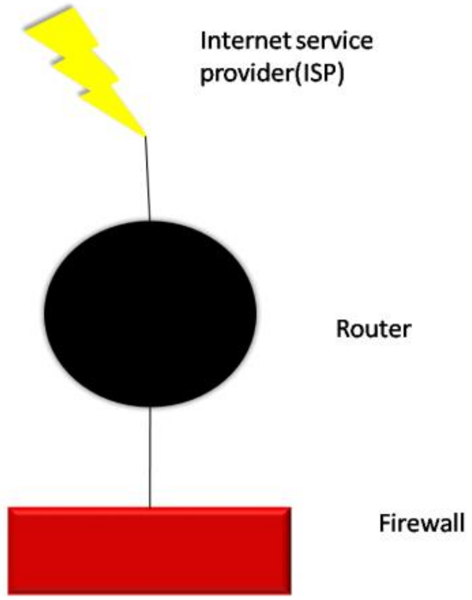
d. Upgrade the WAN links: The upgrade of the WAN links is essential because, according to the company, the current bandwidth seems insufficient. The introduction of new applications along with the existing applications will result in a higher load on the WAN links. After the design is complete, the implementation will be planned, and the design will be implemented.

# Existing Infrastructure:

The Hierarchical is also known as the progressive inter-networking model. This model improves the construction of a structure which is dependable, versatile, and more affordable various leveled internetwork in light of the fact that instead of concentrating on packet construction, it centers around the three functional area, or layers, of your system:

**CORE LAYER:**

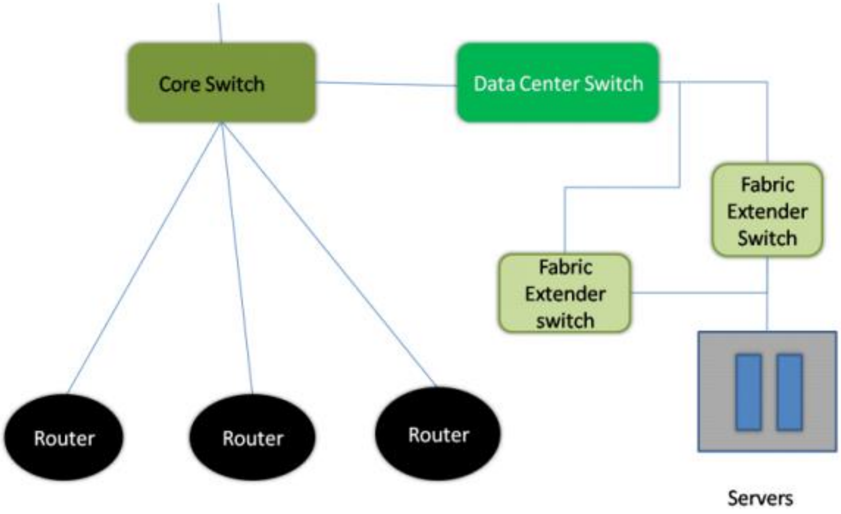
This layer is viewed as the foundation of the system and incorporates the top of the line switches and rapid links or cables, for example, fiber cables. In core layer packets are neither manipulated nor does it route traffic at LAN level. The core layer is solely in charge of quick and dependable transportation of data over a network. The main Aim of this layer is to reduce the latency rate while delivering a packet.



**Core Layer**

**DISTRIBUTION LAYER:**

The distribution layer is in charge of directing the packets. It additionally gives protocol-based network connectivity. It is at this layer where you start to apply authority over network transmissions, incorporating what comes in and what leaves the network. This layer incorporates LAN-based routers and layer 3 switches. This layer guarantees that data packets are legitimately directed among subnets and VLANs in your endeavor. This layer is likewise called the Work-group layer.

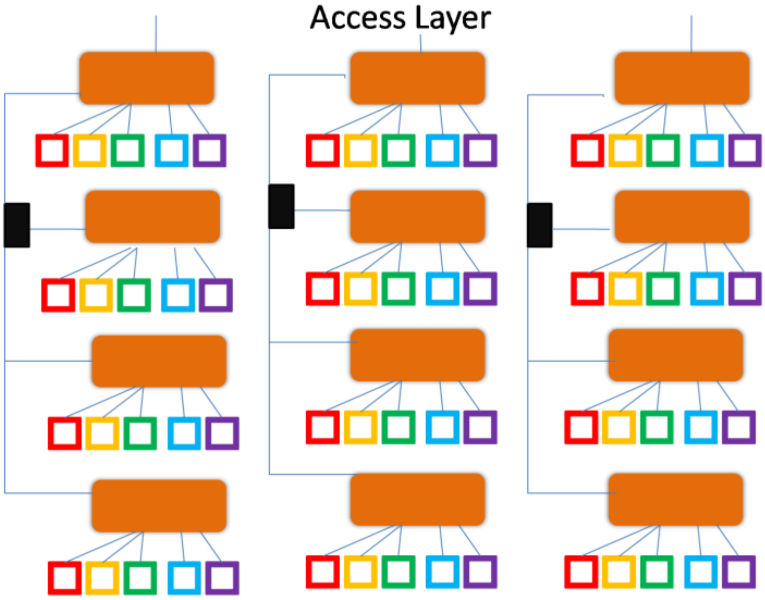


Distribution Layer

## ACCESS LAYER:

The Access layer contains gadgets that permit work-groups and clients to utilize the role played by the core and distribution layers. In the access layer, you can extend or contract network areas utilizing a repeater, standard switch or a hub. This layer is additionally called the work area or desktop layer since it centers around associating end users, for example, computer system to the network. This layer guarantees that data bundles are conveyed to end client PCs.

Access Layer



# Case Study:

## Table of Enterprise Edge:

| | |
|---|---|
| CORE | 3rd floor Admin area and the sales dept. |
| DISTRIBUTION | 1st floor ASA server |
| ACCESS | -1 and 2nd floor pcs in different areas |
| ENTERPRISE EDGE | Client accesses the hospital from an outside network through an ASA firewall. |

The core layer is where the admin has access to his private network along with the information of the entire member's, doctors and employees who work in the hospital.

The distribution layer is placed on the 1st floor is because many people will access, from an outside network to an inside network. Intrusion can also take place here, this can also be considered as the core layer part of the network.

The Access layer contains all the normal floors which includes emergency/mortuary on -1 floor and the patients floor with the doctor's office.

My core layer is highly secure which is located at the 3rd floor of the hospital building which has 2 sections:

i. The Admin Area and
ii. The Sales Area.

The Distribution layer is placed at the 1st Floor which has 2 sections:

i. The ASA (Adaptive Security Appliance),
ii. The Diet Office aka Cafeteria.

The 2nd and -1st Floor of the hospital are normal floors, which are the access layers. 2nd floor has the patient's rooms, and -1 is the mortuary or the emergency floor.

1. The 2nd Floor:
   This floor has 2 parts:
   i. The Doctors office and
   ii. Operation Theatre rooms, normal wards.

## Explanation of Core Layer (3rd Floor):

The admin area is where the Tacacs+ configuration has been implemented because; the admin would have access to his crucial information which only he/she can access with a username and password.

The sales dept. is the area which has all the information about the employees and doctors who work in the hospital, which is ultimately connected to the admin area. This network is internally divided into Vlans (Vlan10, Vlan20, Vlan 30 and Vlan 40). Vlan 30 is connected to a printer. Vlan 40 is an Access Point through which 2 laptops are connected further. So the admin can get all the information about each staff member, nurses and the doctors.

## Explanation of Distribution Layer (1st Floor):

The area where the ASA firewall is configured is implemented there because, that is the part of the hospital where people come and fill the forms and do the payment of money (if any operation/surgery is carried out).

ASA is configured with NAT, DNS. It basically is the ISP.

Waiting place for everyone will also be there, that is why the cafeteria is placed there, where people who are waiting can also take advantage of the delicious food and meals.

Diet Office is an area where food is supplied to the patients on the 2nd floor of the hospital via IP-Phone calls where each phone is assigned a number (1000, 2000, and 3000). These phones can also be accessed by the patients at the 2nd floor.

Since this is where the Kitchen will be, so in case the kitchen catches fire, 4 IoT devices are connected:

1. Cameras: These cameras will work when the Motion detector detects someone coming inside.
2. Motion detector: On when anyone enters or it might be an intruder who tries to enter.
3. Smoke detectors: When smoke more than 1 level is detected the siren automatically starts to beep and the fire sprinkler is automatically on.
4. Siren: Starts when the smoke detector detects more smoke that’s specified in the NTP Server.
5. Fire sprinklers: Starts to water the area when smoke is detected.

## Explanation of Access Layers:

Since this floor is for the OT and normal wards patients, there should be a doctor’s office situated nearby. I have configured a “local login” one for each doctor, this is because every doctor will have a list of patients he/she are treating and the patient’s information in their PC (with their own login and password).

This office is then connected to the 1st floor ASA router, which has all the information of which patient is being treated and has paid and the 1st floor is further connected to the -1 floor /emergency floor.

Patient’s room has a wireless router connected to Laptops in each room for the doctors to give them internet access while they are treating the patients. And each patient’s room has phones connected to the cafeteria on the 1st floor.

Each phone is assigned a number (100, 200, and 300).

The mortuary/Emergency floor is where 2 cars are acting as ambulance’s, an emergency door (which is always open).

An Access point which gives internet to many devices which is turn connected to a server (FTP AND SMTP) . This floor device give all the details to the first floor trough the FTP or SMTP servers used devices making them aware who entered the emergency room and various kind of information’s.

# Network Devices:

**Router:** In our network we have routers at two levels, one at the core level and one at the distribution layer. We need to handle the bandwidth of 100mbps for now. To handle this bandwidth we are choosing Cisco 4351 router at the core layer. The reasons behind choosing it are:

- Cisco 4351 can smoothly give throughput of 200mbps.
- It can be upgraded to 400mbps if required.
- It has 3 onboard LAN/WAN ports.
- It has 48 Maximum switched Ethernet ports.

**Core Switch:** Core switch comes at the top of distribution switch. It is also known as tandem switch or backbone switch. The main role of core switch in our network is to increase the speed of delivering data packets in the centre of network. Here for our network we have chosen Cisco 6000 series. The reasons behind doing so are:

- It has very less failure rate.
- It has very high scalability.
- Upgradable.

**Data Centre Switch:** The data centre switch is emerging as a new class of switch since data centre networking infrastructures become more disaggregated. Unlike the network switch for traditional three-tier hierarchical networks, data centre class switches are designed to support data and storage for mission critical applications. Here we have chosen Cisco 5548 data centre switch and the reasons behind having a data centre switch in our network are:

- They can handle both north-south and east-west traffic flows.
- They support high-bandwidth interconnections using both standard LAN Ethernet protocol and SAN protocols. For example, Fibre Channel and Fibre Channel over Ethernet.
- They have extensive high availability and fault tolerance systems in the hardware and software. Therefore provide better uptime for mission-critical applications.

**Fabric Extender Switch**: In our network we have chosen this fabric extender purely for future use. As hospital is planning to build two more blocks and if government plan to connect different district level hospitals then traffic will be huge while accessing servers.

**ISP:** A network is of little of no use without internet. For the project as big as this consisting almost 400-500 end users accessing internet at the same time we need a high speed internet service provider. We cannot compromise on internet speed as people life’s on stack. Here we choose a connection of 100mbps bandwidth from a reputed Internet Service Provider. The reasons behind doing so are:

- Providing high speed internet for uninterrupted high quality video communication in various operation theatres.
- Various hospital employees accessing working on their workstations at the same time.
- Providing fixed bandwidth for visitors as they might surf videos or browse sites while waiting in the waiting area.
- Considering near future expendability.

**Firewall:** Firewall is a system designed to prevent unauthorized access to or from a private network. Firewall prevents unauthorized internet users to access private network connected to internet, especially intranet. All the packets coming or leaving the network has to pass through firewall. It checks and examines every data packets and prevents access if fails to meet security criteria set by the network admin. Firewall can be implemented both at hardware and software level. Here we have installed packet filtering firewall and web application firewall. Former will examine the data packets and later will allow only specific web application to be used by the employees. Our router is capable of filtering the data packets and restricts web applications according to the protocols configured by the admin.

**Server:** Server is a central system used for storing and managing data of entire network. Here in our network we have installed three dedicated server i.e. FTP server, mail server, web server.

**Hub:** In a network, a hub is a port that broadcasts to every end device or Ethernet-based device connected to it. Here in our model we used hubs to connect switches of different floor. The reason behind doing is to increase the reliability. We can easily figure out the fault if any floor is not receiving internet connection.

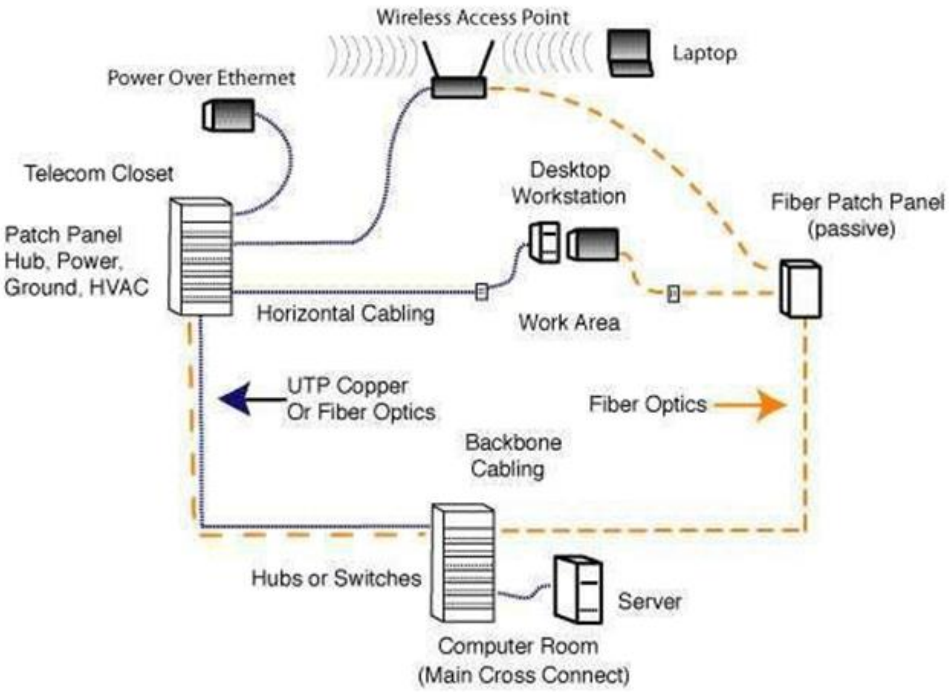
**Wireless Access Point (WAP):** Wireless Access Points are basically devices which allow wireless devices to connect with either the help of WI-FI or Bluetooth medium. We are using two WAP at each floor to provide maximum internet connectivity to wireless medical devices, smart phones, smart mobile tablets, laptops, etc

**Access Switches:** Access switches come at the Access layer of a network. It brings the distribution network inside the building. It is the most commonly used gigabit Ethernet switch which communicates directly with public internet. These switches are responsible for establishing connection with end devices like computers, laptops, mobile phones with both wired and wireless medium. Here in our network we have used one access switch at every floor of our building. In our network we have used Cisco 4510 idf's. The reasons behind it are:

- Number of ports.
- High performance.
- Great efficiency.

**Cables**: Last but also the very important part is cabling the entire network. Without connecting one component of a network with other it is pretty much useless. Here in our model we had used Unshielded Twisted Pair (UTP) cables to connect network to router, routers to switch, switch to servers, switch to end devices. WE chose UTP cables because of its interference cancelling capabilities. To be very particular we used cat-6 grade cables because of its maximum transmission speed of 1000mbps/100 meters. There is not much cost difference between cat5e and cat-6 grade cable. So it is a vice choice to choose cat-6 cable for our network.

**Virtual LANS:** A VLAN is a logical grouping of network users and resources connected to administratively defined ports on a switch. When VLANs are created, it becomes possible to create smaller broadcast domains within a layer 2 switched internetwork by assigning different ports on the switch to service different subnetworks. A VLAN is treated like its own subnet or broadcast domain, meaning that frames broadcast onto the network are only switched between the ports logically grouped within the same VLAN.



Wireless Connection of a Network

# **Request for Proposal (RFP):**

## Project Overview:

This work is related to a project that uses networking in hospitals and has examined various recommendations and techniques for using the hospital network's private addressing schemes. We switched quickly between the LANs and ensured a secure WLAN network was provided. This will contribute to health promotion, which together with patient safety and clinical effectiveness is a core dimension of quality in hospital services.

## Project Goals:

We need to design a network topology that is easy to understand, easy to manage, easy to troubleshoot and is adaptable to change in future according to the new medical equipment. Among the various topologies like bus topology, ring topology, mesh topology, star topology, etc, Hierarchical topology would best meet our demands.

In general, in designing and maintaining the performance, efficiency, architecture and security of the hospital network, the IT manager faces a lot of challenges. An important consideration of network design for today's networks is creating the potential to reliably, scalably and securely support future expansion.

## Scope of Work:

This study will dissect and analyze different parts of the network of a hospital, uncovering substandard practices and problematic weaknesses that commonly result in a general decline in the quality of healthcare provided to patients, and adversely affecting hospital and healthcare facilities' business operations.

# Remote Site Connectivity:

Objective: Provide a unified solution for connection purpose
Grant the connection seamlessly, as if in company headquarters Application requirements include:

- Low to medium-volume data files transfer and interactive traffic for sender and receiver.
- Connectivity option: IP access through an on-demand or always-on connection.
- Technologies include DHCP, RIP and Wireless.

Lightweight access point designed to be controlled across WAN links: –REAP is designed to support remote offices by extending LWAPP control timers.

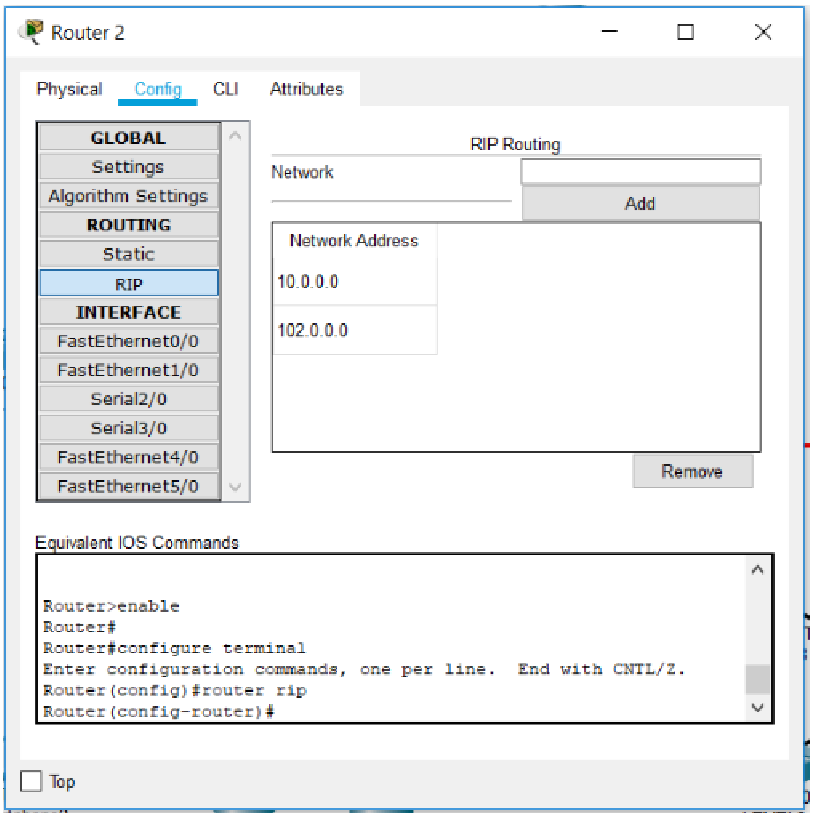
- Control traffic is still LWAPP encapsulated and sent to Cisco Wireless LAN Controller.
- Client data is not LWAPP-encapsulated but is locally bridged.

All management control and RF management is available when the WAN link is up and connectivity is available to the Cisco Wireless LAN Controller. It will continue to provide local connectivity even if the WAN is down.

### Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network.

Routing Information Protocol (RIP) is a protocol that routers can use to exchange network topology information. It is characterized as an interior gateway protocol, and is typically used in small to medium-sized networks. The routing table is broadcast to all stations on the attached network.



Network Address: 10.0.0.0, 102.0.0.0

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#
```

## Connectivity:

I have used the 5 connectivity types in my network.

- Copper Straight- through,
- Serial DCE (for connecting 2 or more router’s),
- Copper Cross Over (Switch to Switch),
- IoT Custom Cable (for the IoT device connectivity) and
- Console

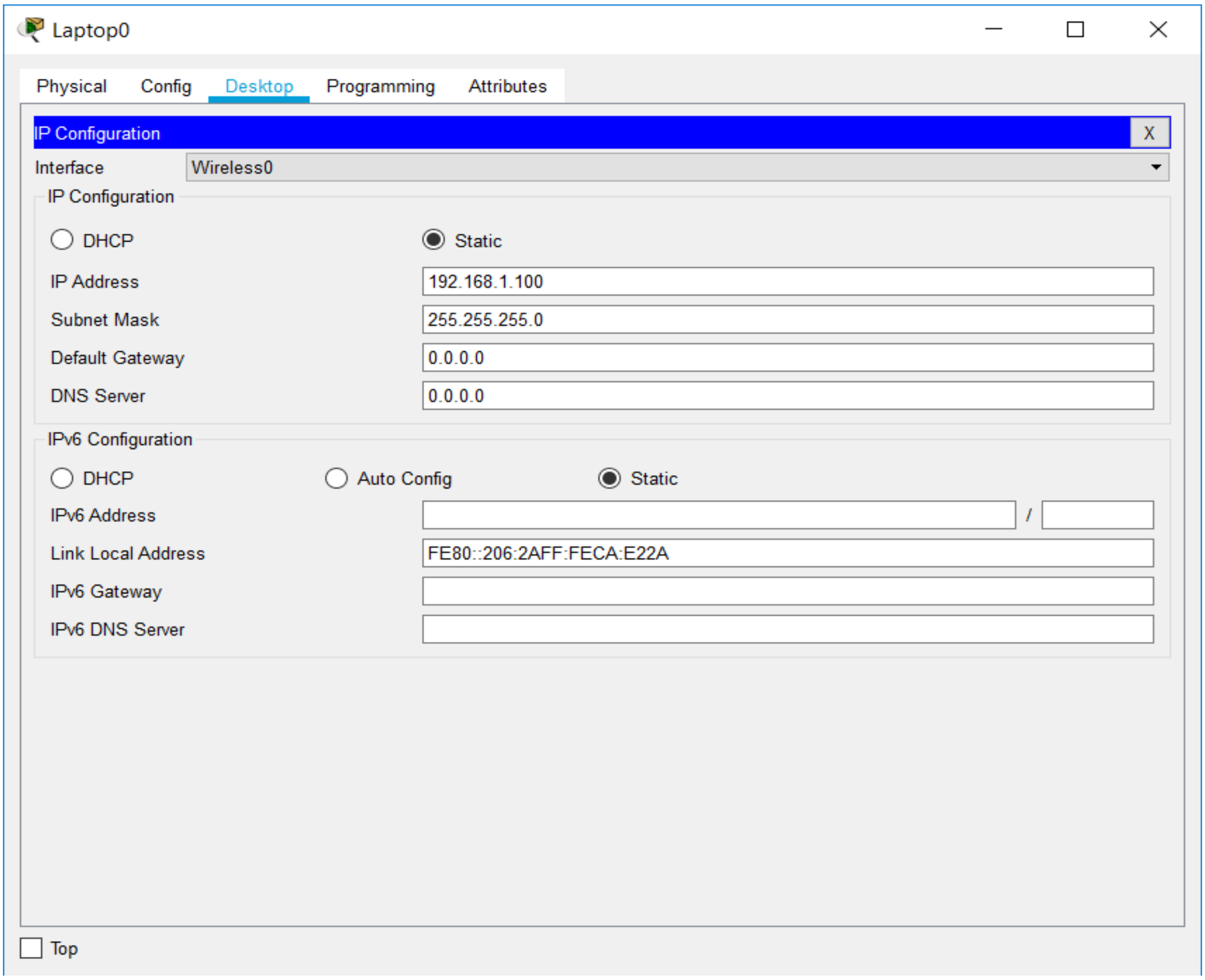
## Security:

SSH, tacacs+, asa firewall, local login, vlans.

# IP Addressing Plan:

## Static IP Address

A static Internet Protocol (IP) address (static IP address) is a permanent number assigned to a computer by an Internet service provider (ISP). Static IP addresses are useful for gaming, website hosting or Voice over Internet Protocol (VoIP) services. Speed and reliability are key advantages. Because a static address is constant, systems with static IP addresses are vulnerable to data mining and increased security risks.
A static IP address is also known as a fixed address. This means that a computer with an assigned static IP address uses the same IP address when connecting to the Internet.



IP Configuration

Interface: Wireless0

IP Configuration

○ DHCP ● Static

IP Address: 192.168.1.100

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address: /

Link Local Address: FE80::206:2AFF:FECA:E22A

IPv6 Gateway:

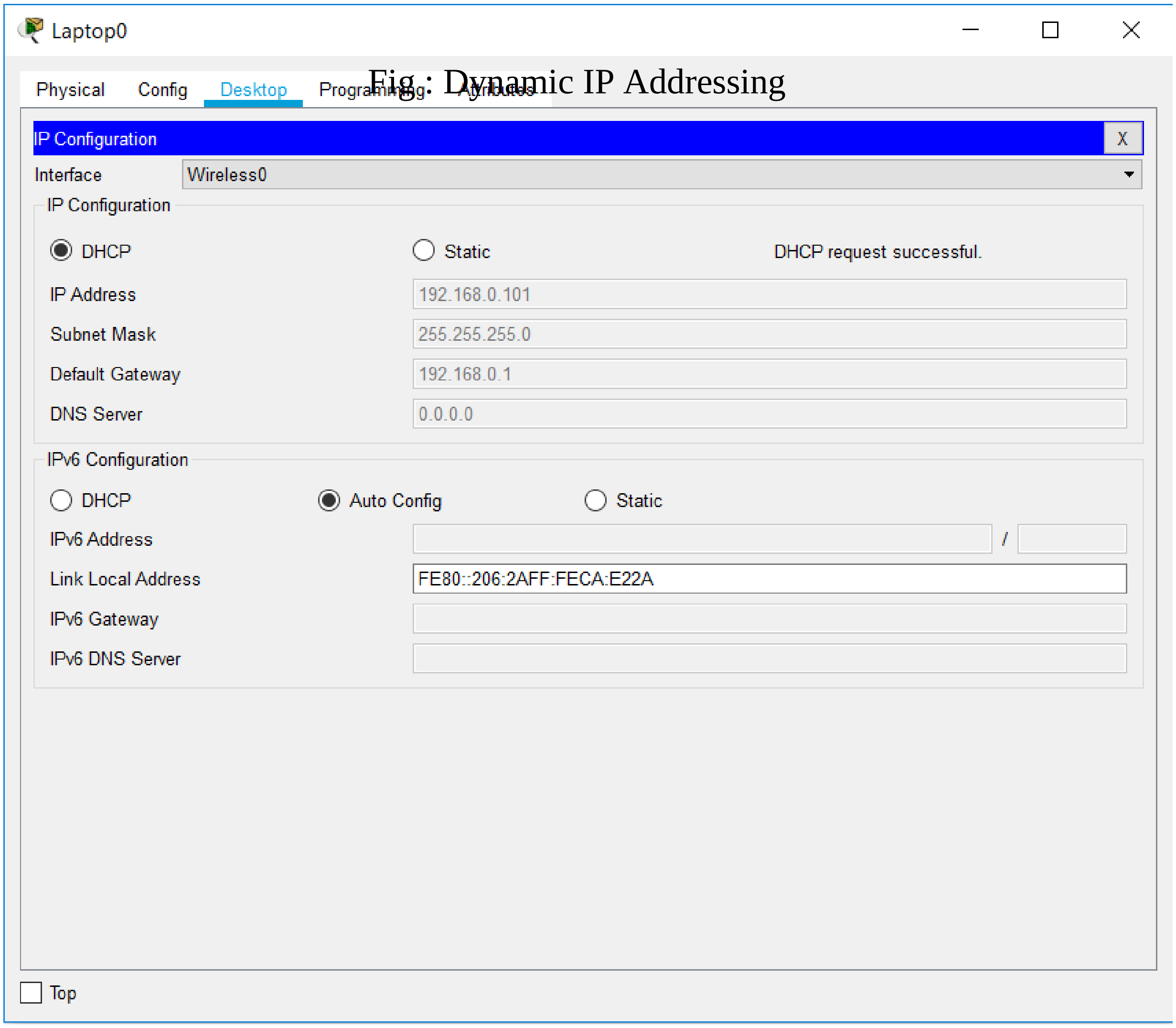
IPv6 DNS Server:

□ Top

Fig: Static IP Addressing

# Dynamic IP Address

A dynamic Internet Protocol address (dynamic IP address) is a temporary IP address that is assigned to a computing device or node when it's connected to a network. A dynamic IP address is an automatically configured IP address assigned by a DHCP server to every new network node.



IP Configuration

Interface: Wireless0

IP Configuration

● DHCP ○ Static DHCP request successful.

IP Address: 192.168.0.101

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ DHCP ● Auto Config ○ Static

IPv6 Address: /

Link Local Address: FE80::206:2AFF:FECA:E22A

IPv6 Gateway:

IPv6 DNS Server:

Fig.: Dynamic IP Addressing

# Routing Protocol Plan:

In my Network I have used

i. FTP:
Used for file transferring between 2 different networks.

ii. SMTP(Emails):
Used for sending emails.

iii. NTP:
Used for the IoT devices used as well as the local storage of data. This shows the current time and data on the IP-Phones used .

iv. SSH(Local Login):
Used so that for every doctor there is a separate username and password when the doctor enters his/her office.

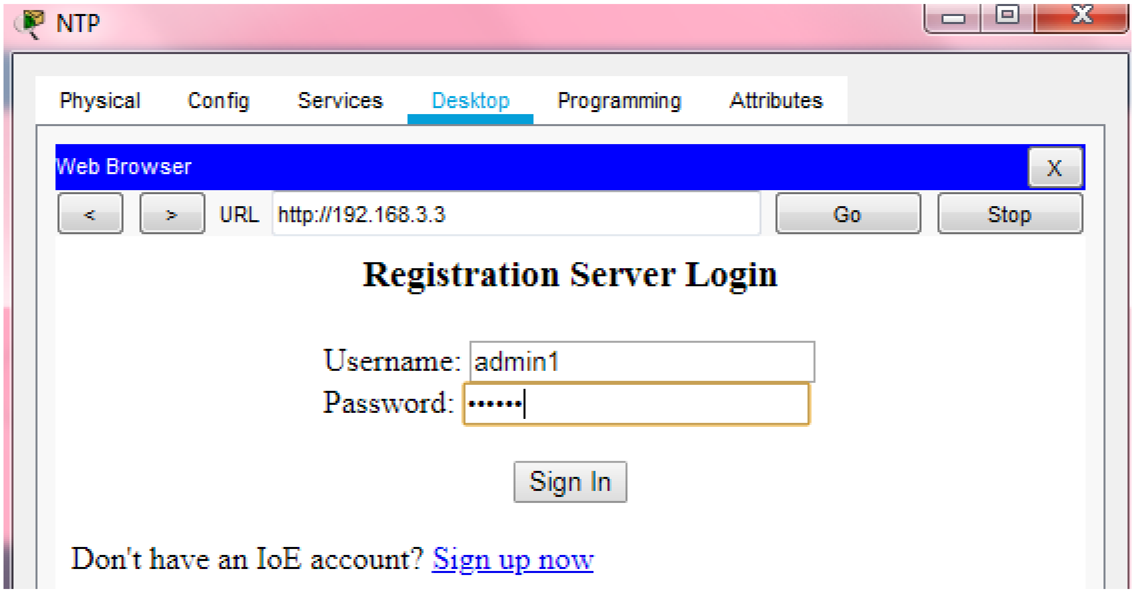
v. AAA(tacacs+):
Crucial admin data are stored here which only one person knowing the password can access.

vi. VLAN:
Vlans are used for security internally among the same network.

vii. RIP:
Used for communicating between 2 networks.

viii. NAT:
Used with the ASA firewall because people will access the hospital via the outside public network which the NAT translates and the firewall scans the packet before allowing the packet to enter.

## NTP:



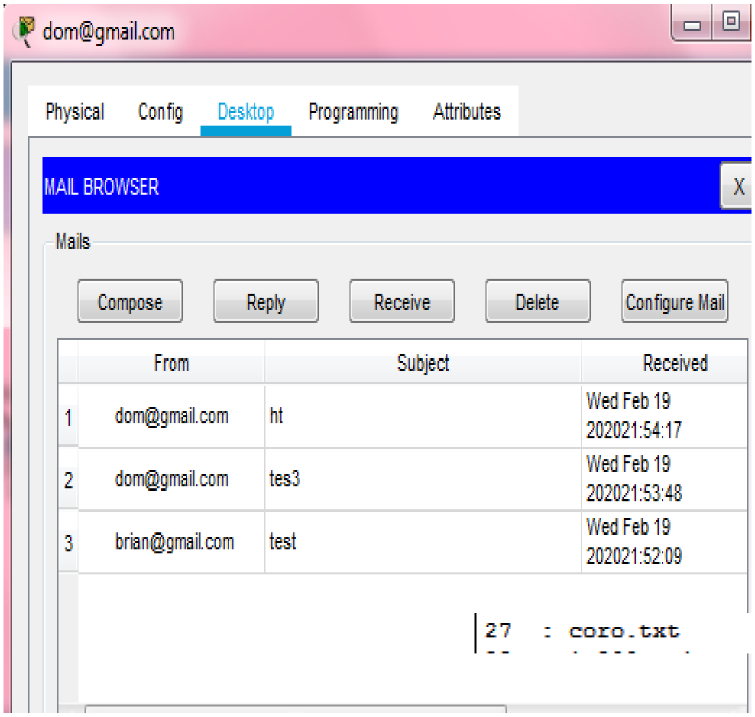
URL http://192.168.3.3

Registration Server Login

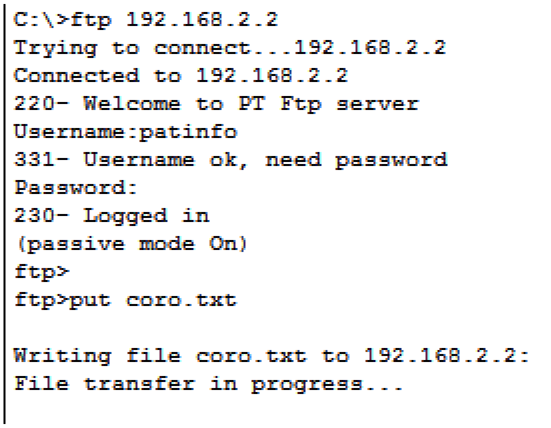
Username: admin1
Password: ••••••

Don't have an IoE account? Sign up now

## FTP AND SMTP:



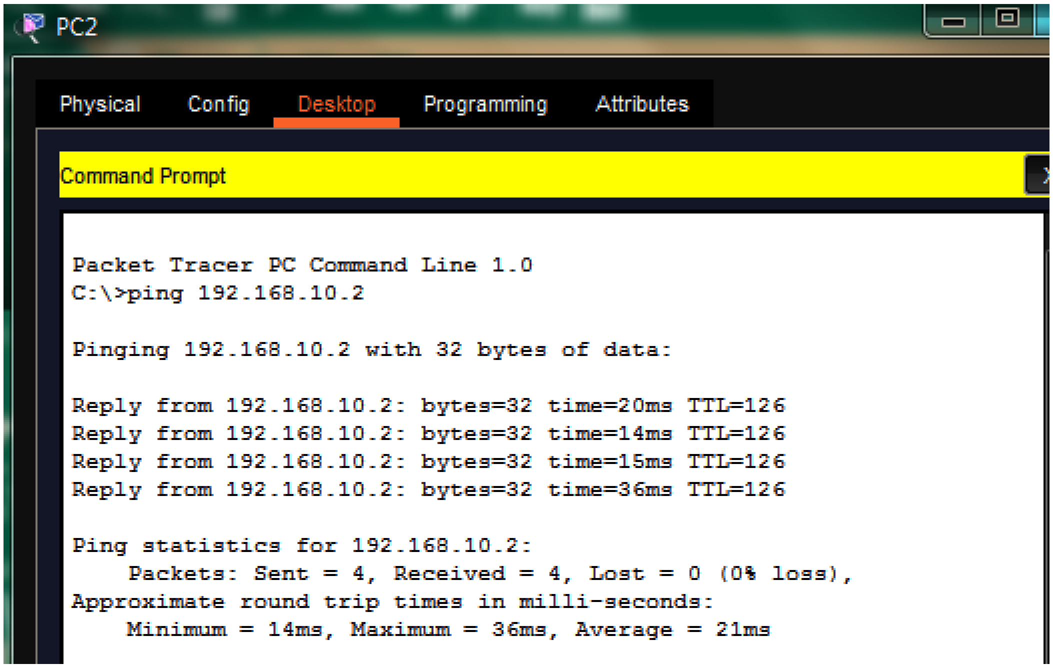
| | From | Subject | Received |
|---|---|---|---|
| 1 | dom@gmail.com | ht | Wed Feb 19 202021:54:17 |
| 2 | dom@gmail.com | tes3 | Wed Feb 19 202021:53:48 |
| 3 | brian@gmail.com | test | Wed Feb 19 202021:52:09 |



```
C:\>ftp 192.168.2.2
Trying to connect...192.168.2.2
Connected to 192.168.2.2
220- Welcome to PT Ftp server
Username:patinfo
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
ftp>put coro.txt

Writing file coro.txt to 192.168.2.2:
File transfer in progress...
```

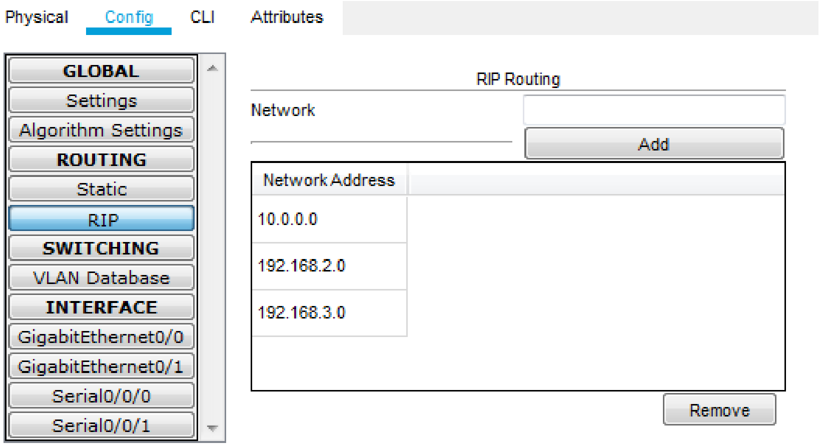
```
27  : coro.txt                                          79
```

ASA: from PC2 to Server



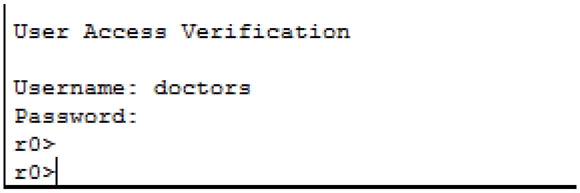
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=20ms TTL=126
Reply from 192.168.10.2: bytes=32 time=14ms TTL=126
Reply from 192.168.10.2: bytes=32 time=15ms TTL=126
Reply from 192.168.10.2: bytes=32 time=36ms TTL=126

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 36ms, Average = 21ms
```

# RIP



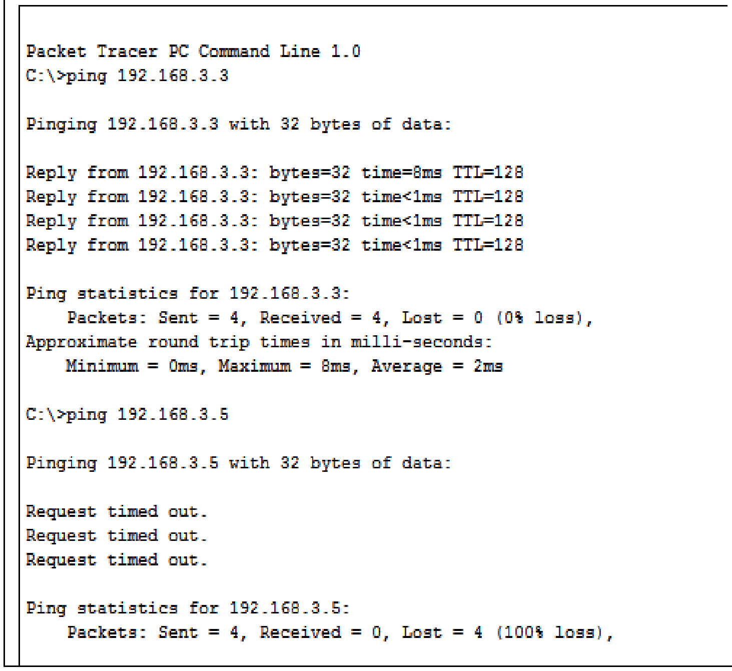
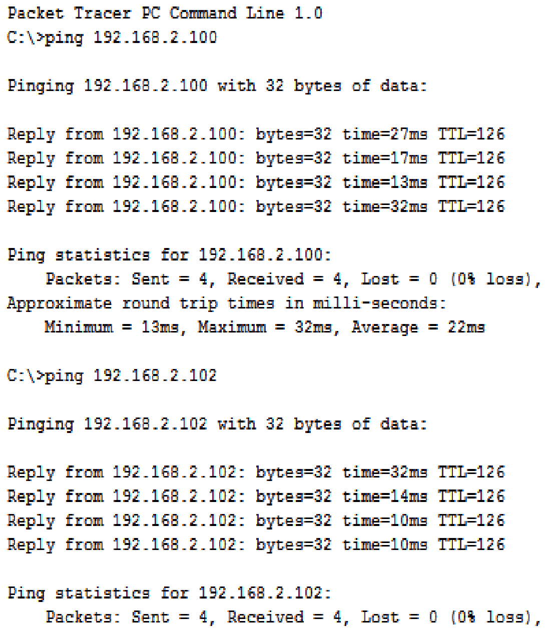
| Network Address |
|---|
| 10.0.0.0 |
| 192.168.2.0 |
| 192.168.3.0 |

# LOCAL LOGIN



```
User Access Verification

Username: doctors
Password:
r0>
r0>
```

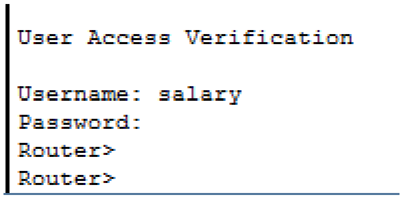
## VLAN 10,20,30:

| Ping from same vlan pcs and 2nd ping from pcs in different vlans | When pc pings to the patients laptops |
|---|---|
|  |  |

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=8ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 8ms, Average = 2ms

C:\>ping 192.168.3.5

Pinging 192.168.3.5 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.3.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.100

Pinging 192.168.2.100 with 32 bytes of data:

Reply from 192.168.2.100: bytes=32 time=27ms TTL=126
Reply from 192.168.2.100: bytes=32 time=17ms TTL=126
Reply from 192.168.2.100: bytes=32 time=13ms TTL=126
Reply from 192.168.2.100: bytes=32 time=32ms TTL=126

Ping statistics for 192.168.2.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 32ms, Average = 22ms

C:\>ping 192.168.2.102

Pinging 192.168.2.102 with 32 bytes of data:

Reply from 192.168.2.102: bytes=32 time=32ms TTL=126
Reply from 192.168.2.102: bytes=32 time=14ms TTL=126
Reply from 192.168.2.102: bytes=32 time=10ms TTL=126
Reply from 192.168.2.102: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.2.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

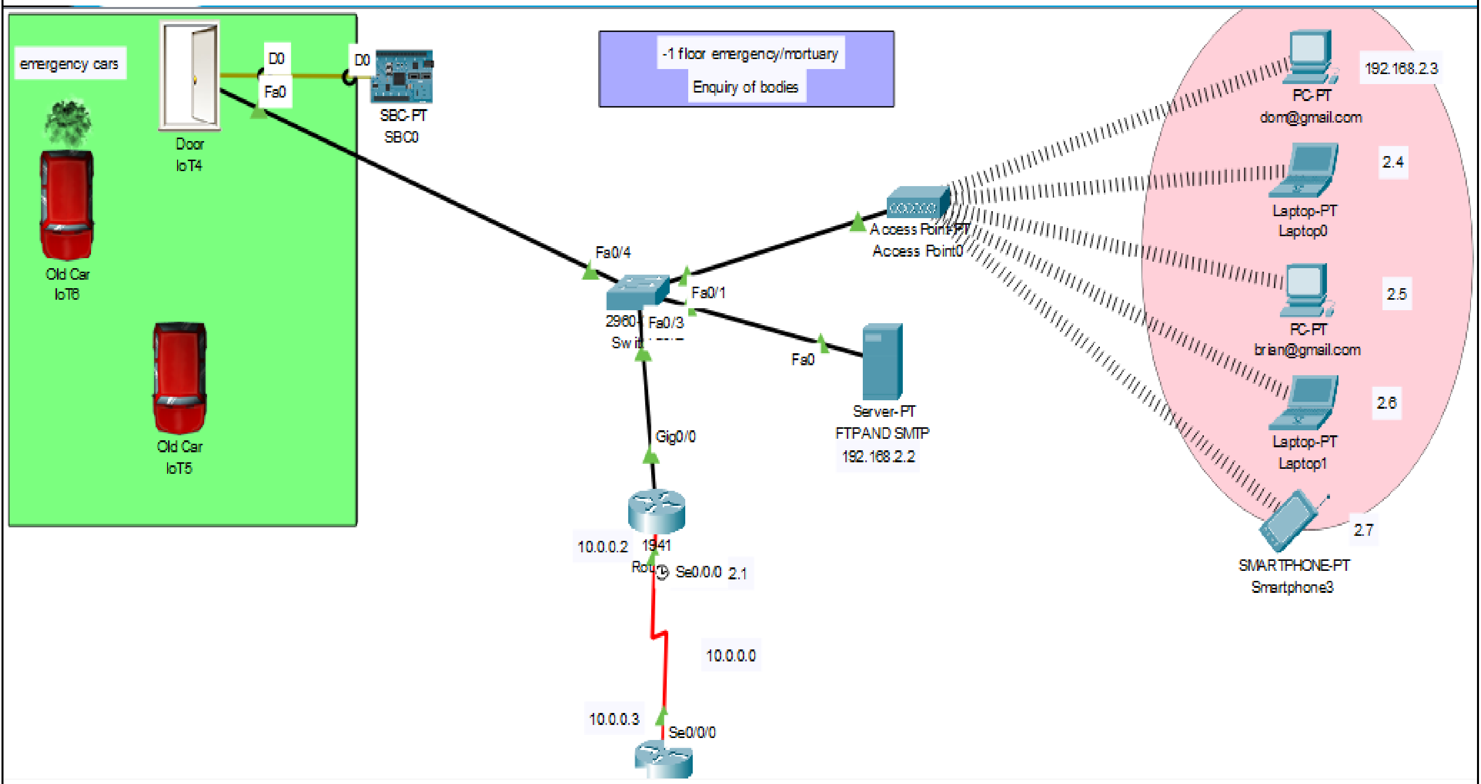
## TACACS+



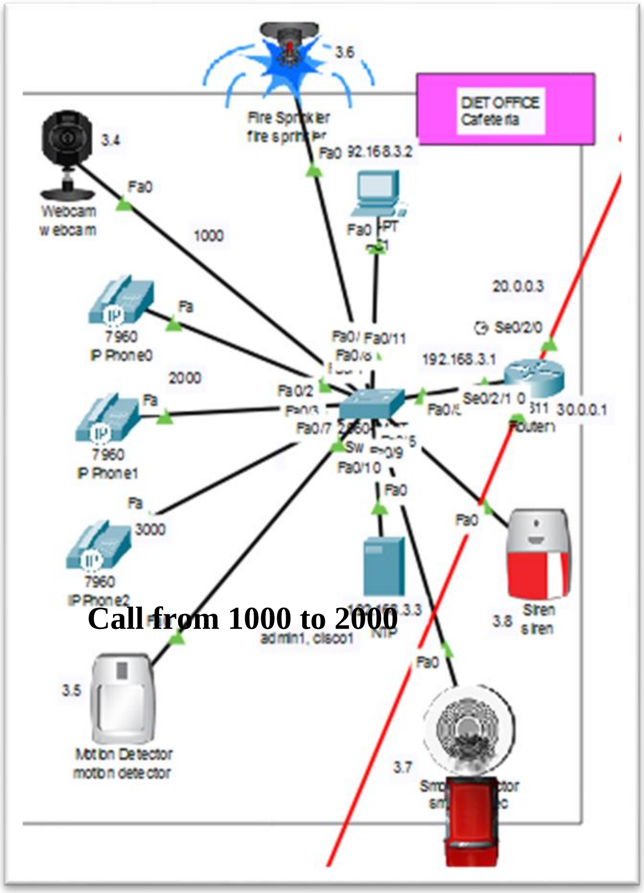
```
User Access Verification

Username: salary
Password:
Router>
Router>
```

# <u>Network Design</u> (Topology):

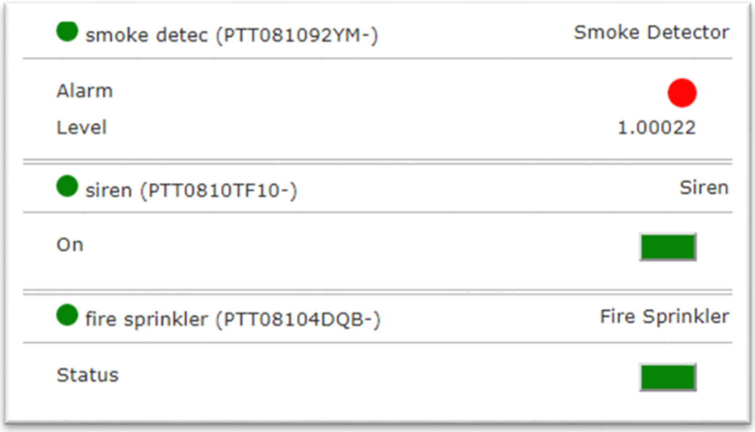
My Topology basically starts with -1 floor followed by the 1st floor and so on…



# 1st Floor :



Call from 1000 to 2000



● smoke detec (PTT081092YM-) Smoke Detector

Alarm ●

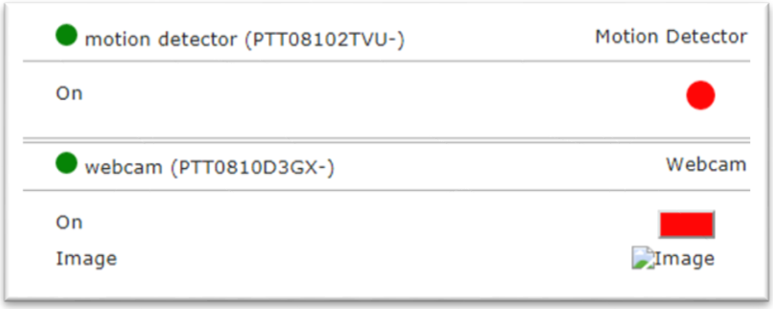
Level 1.00022

● siren (PTT0810TF10-) Siren

On 🟩

● fire sprinkler (PTT08104DQB-) Fire Sprinkler

Status 🟩



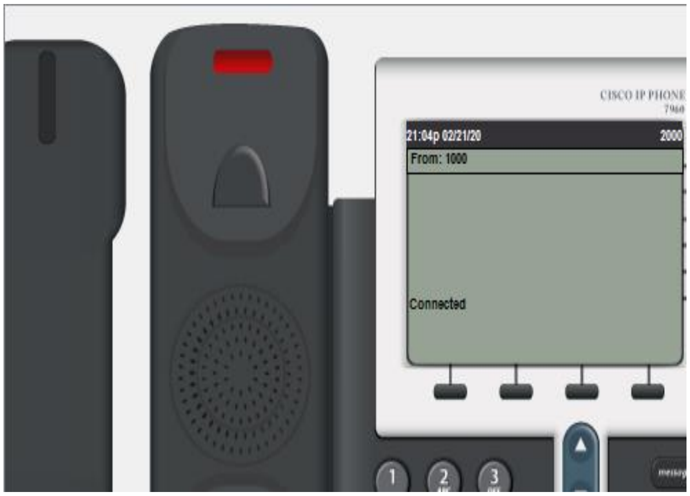
● motion detector (PTT08102TVU-) Motion Detector

On ●

● webcam (PTT0810D3GX-) Webcam

On 🟥

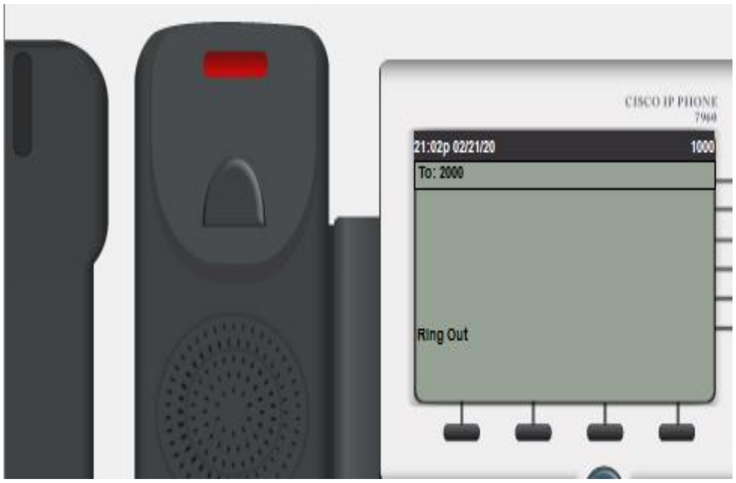
Image Image



21:04p 02/21/20 2000

From: 1000

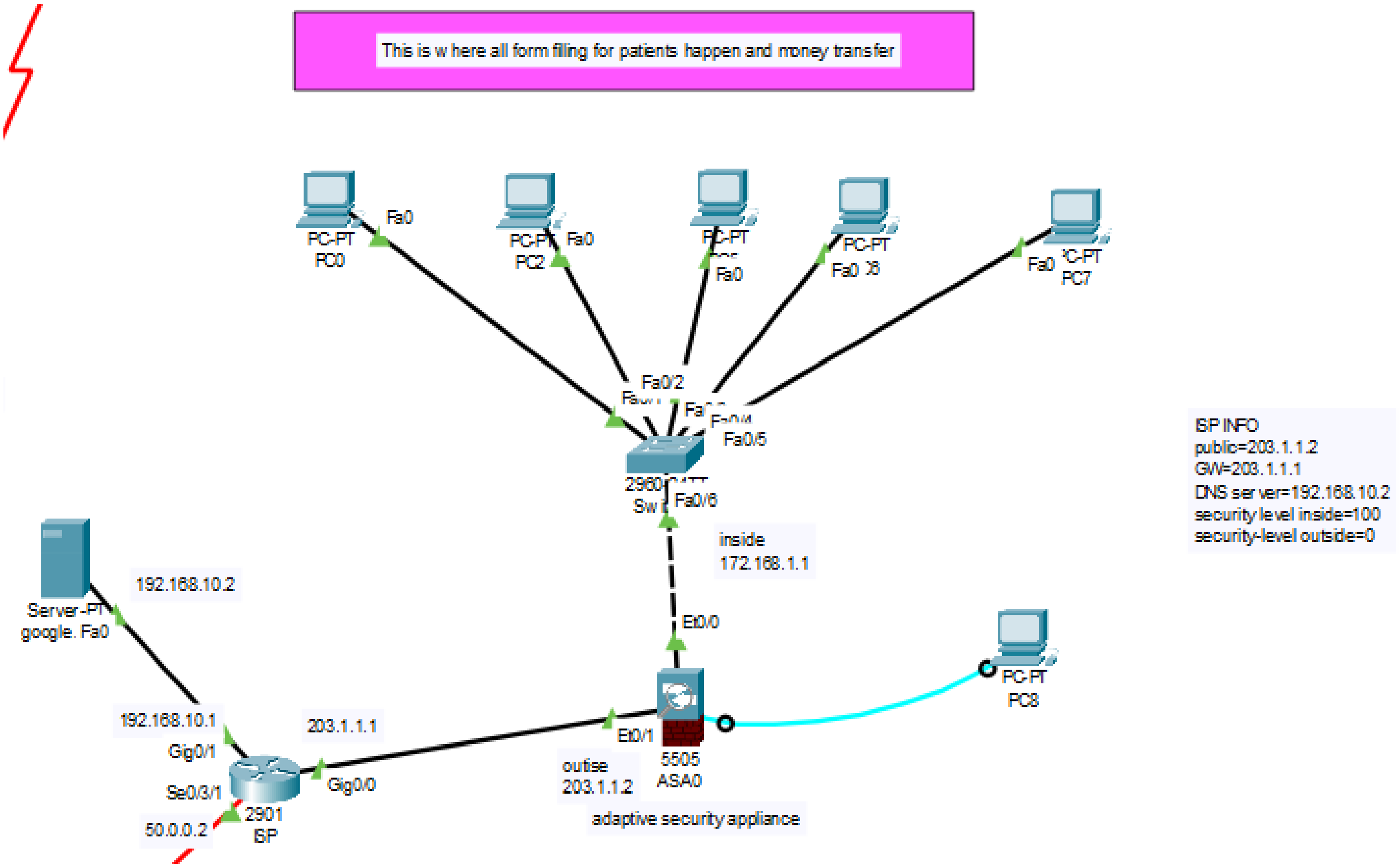
Connected



21:02p 02/21/20 1000

To: 2000

Ring Out



This is w here all form filling for patients happen and money transfer

ISP INFO
public=203.1.1.2
GW=203.1.1.1
DNS ser ver=192.168.10.2
security level inside=100
security-level outside=0

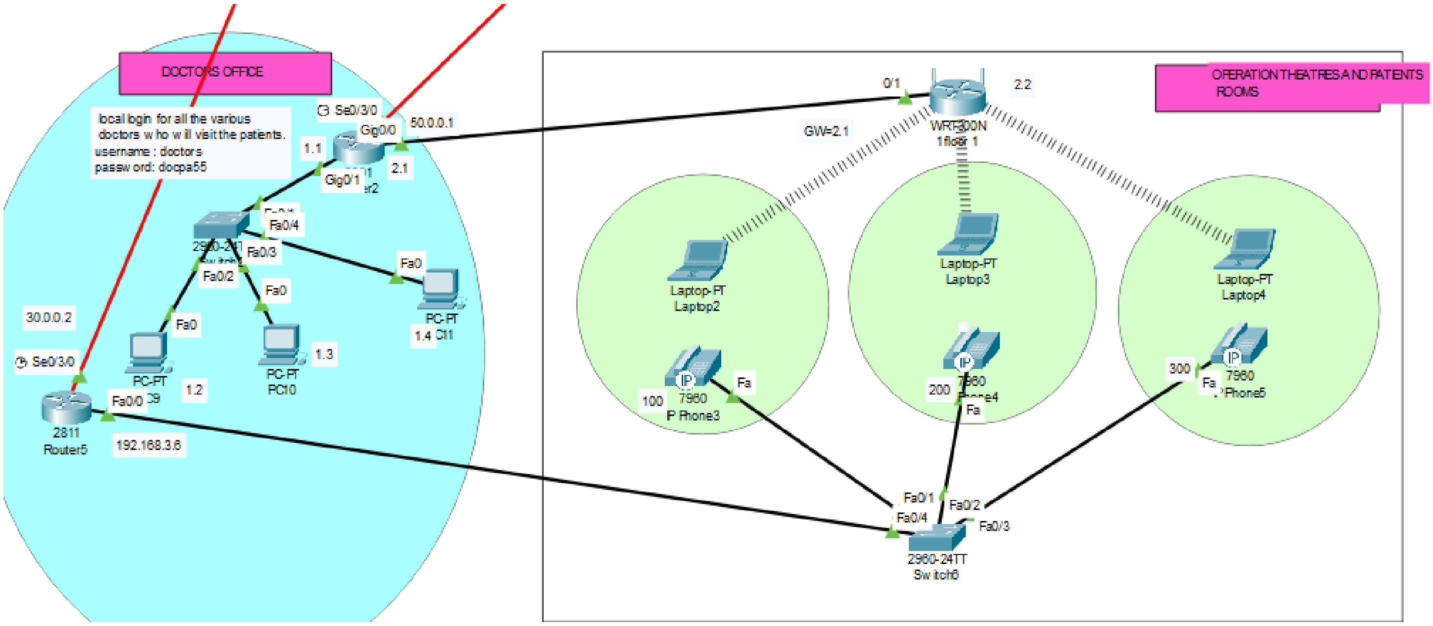
inside
172.168.1.1

192.168.10.2

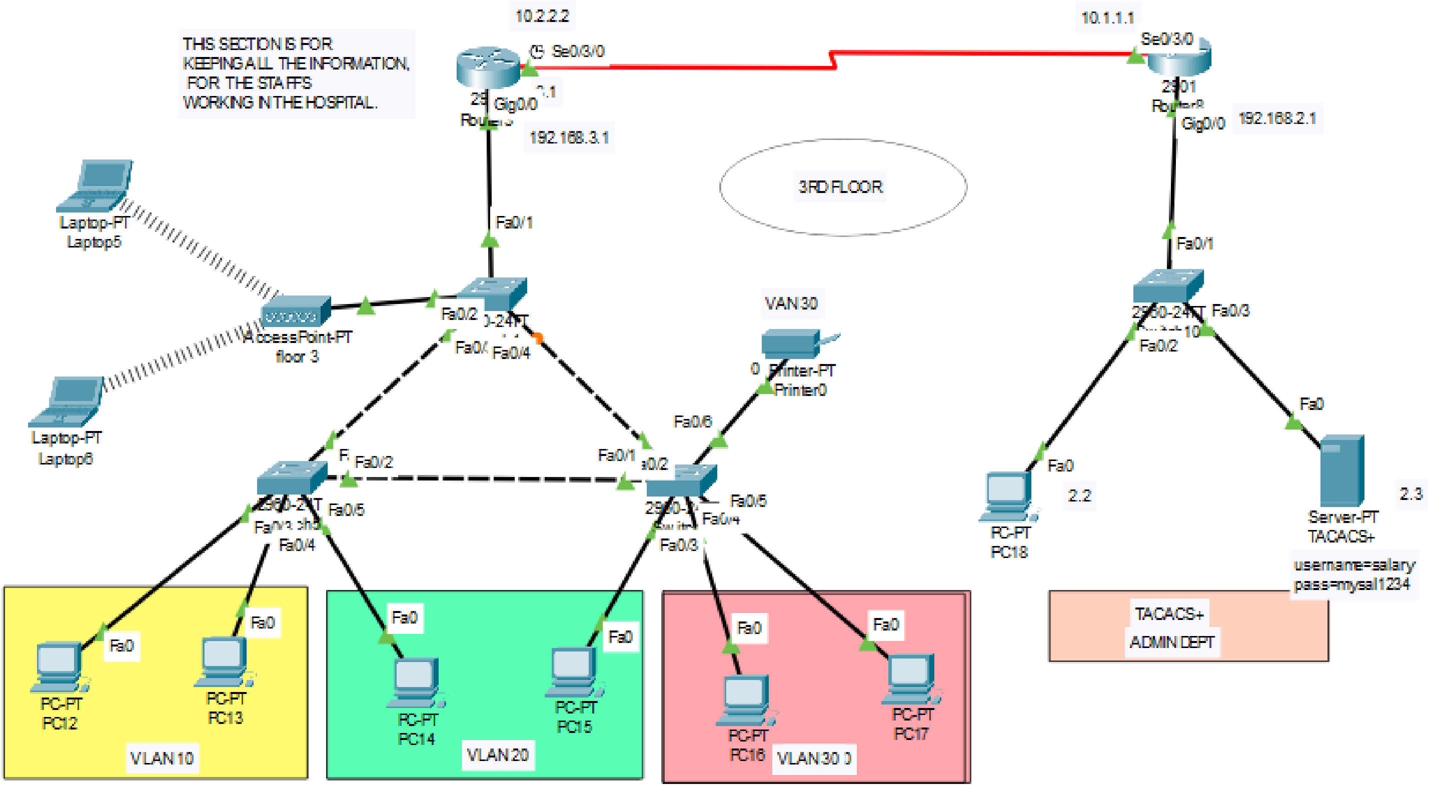
outise
203.1.1.2

adaptive security appliance

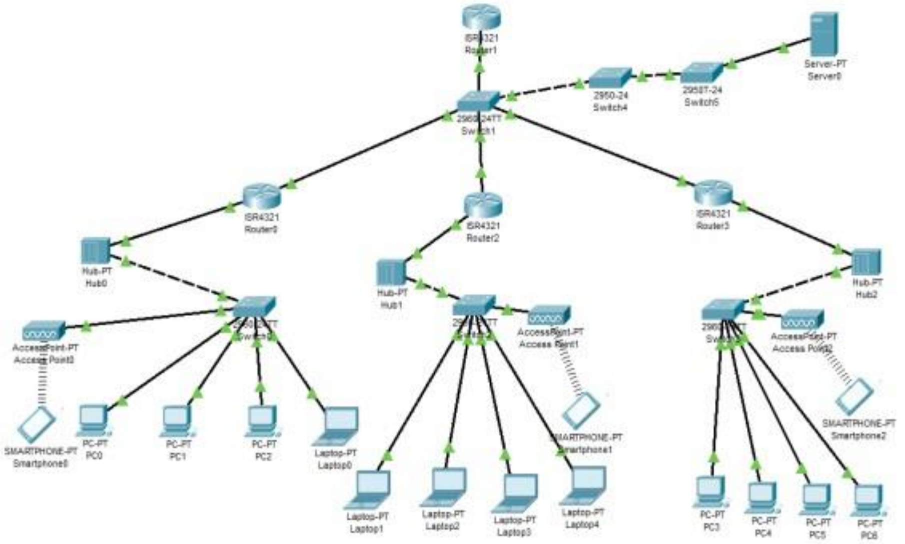
# 2$^{nd}$ Floor:


DOCTORS OFFICE
local login for all the various doctors w ho w ill visit the patients.
username : doctors
passw ord: docpa55
Se0/3/0
Gig0/0
50.0.0.1
1.1
2.1
Gig0/1
er2
Fa0/4
2960-24T
Fa0/3
Fa0/2
Fa0
Fa0
Fa0
PC-PT
1.4
PC-PT
PC10
1.3
PC-PT
1.2
30.0.0.2
Se0/3/0
Fa0/0
2811
Router5
192.168.3.6
0/1
2.2
WRT300N
1floor 1
GW=2.1
OPERATION THEATRES AND PATIENTS ROOMS
Laptop-PT
Laptop2
Laptop-PT
Laptop3
Laptop-PT
Laptop4
100
7960
IP Phone3
Fa
200
7960
Phone4
Fa
300
Fa
7960
Phone5
Fa0/1
Fa0/2
Fa0/4
Fa0/3
2960-24TT
Sw itch6

# 3rd Floor:


10.2.2.2
THIS SECTION IS FOR
KEEPING ALL THE INFORMATION,
FOR THE STAFFS
WORKING IN THE HOSPITAL.
Se0/3/0
Gig0/0
192.168.3.1
10.1.1.1
Se0/3/0
2901
Gig0/0
192.168.2.1
3RD FLOOR
Laptop-PT
Laptop5
Laptop-PT
Laptop6
AccessPoint-PT
floor 3
Fa0/1
Fa0/2
Fa0/4
VAN 30
Printer-PT
Printer0
Fa0/6
Fa0/1
Fa0/2
Fa0/5
Fa0/4
Fa0/3
Fa0/4
Fa0/5
2960-24TT
Fa0/1
2960-24TT
Fa0/3
Fa0/2
Fa0
Fa0
2.2
2.3
PC-PT
PC18
Server-PT
TACACS+
username=salary
pass=mysal1234
TACACS+
ADMIN DEPT
Fa0
Fa0
PC-PT
PC12
PC-PT
PC13
VLAN 10
Fa0
Fa0
PC-PT
PC14
PC-PT
PC15
VLAN 20
Fa0
Fa0
PC-PT
PC16
PC-PT
PC17
VLAN 30

# IMPLEMENTATION



# Conclusion:

With the growth of Information Technology in every sector and the explosion of medical IOT devices, the design of a network of any hospital has become very essential factor. The hospitals need to have a reliable, secure and scalable network design in order to keep the patients information, doctor's research work safe, convenient communication between various departments, etc. as well as keep it ready for any new IOT medical equipments that may be introduced in the future. The hierarchical model of networking best suits our needs along with providing additional features like easy maintenance, high security, simplified troubleshooting and effective performance

# Bibliography:

[1]-The Hospital Network - A New Approach Towards Networking Zeeshan Ahmed Siddique

[2]-Hospital Network Infrastructure: a Modern Look Into the Network Backbone with Real Time Visibility Homan Mike Hirad