**Secure Hospital Area Network Design**

Ashish Sapkota

LC00017001073

TEXAS COLLEGE OF MANAGEMENT & IT



DEPARTMENT OF CYBER SECURITY AND NETWORKING

LINCOLN UNIVERSITY COLLEGE

SEPTEMBER 27TH, 2023

**Declaration**

I, Ashish Sapkota, solely 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 and Data 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.

**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 Secure hospital network that 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 a secured LAN and WLAN network. The network is designed by keeping in mind upcoming technology in the medical field. This will increase the quality of hospital service along with patient safety and clinical effectiveness.

**Acknowledgement**

I would like to extend my heartfelt gratitude to my friends and teachers who have provided invaluable support and guidance throughout my thesis journey. I would like to express my sincere appreciation to my friends, who have been a constant source of motivation and encouragement. Their unwavering support, understanding, and belief in me have helped me stay focused and overcome the challenges I faced.

I am also deeply grateful to my teachers for their invaluable contributions. Their expertise and guidance have been instrumental in shaping my research and bringing my thesis to fruition. Their patience, support, and feedback have been invaluable, and I am truly honored to have had the opportunity to learn from such accomplished professionals. Finally, I would like to thank my family, who have provided me with unending love, support, and encouragement throughout my academic journey. Their unwavering belief in me has been the driving force behind my success, and I am forever grateful for their love and support. Thank you all for being an integral part of my thesis journey. Your support and guidance will always be remembered and cherished.

Contents

[Introduction 6](#_Toc146846419)

[Objectives: 7](#_Toc146846420)

[Scope of the Project: 7](#_Toc146846421)

[Background Study and Literature Review: 8](#_Toc146846422)

[Project Planning: 11](#_Toc146846423)

[Working Methodology: 11](#_Toc146846424)

[1) CORE LAYER 11](#_Toc146846425)

[2) DISTRIBUTION LAYER 12](#_Toc146846426)

[3) ACCESS LAYER 12](#_Toc146846427)

[Major Design Areas & Functional Areas: 13](#_Toc146846428)

[Network Devices 14](#_Toc146846429)

[Router 14](#_Toc146846430)

[Core Switch 14](#_Toc146846431)

[Data Centre Switch 15](#_Toc146846432)

[Fabric Extender Switch 15](#_Toc146846433)

[ISP 15](#_Toc146846434)

[Firewall 16](#_Toc146846435)

[Server 16](#_Toc146846436)

[Wireless Access Point (WAP): 16](#_Toc146846437)

[Cables 17](#_Toc146846438)

[Virtual LANS 17](#_Toc146846439)

[Implementation and Testing: 18](#_Toc146846440)

[Explanation of Core Layer (3rd Floor): 18](#_Toc146846441)

[Explanation of Distribution Layer (1st Floor): 18](#_Toc146846442)

[Explanation of Access Layers: 18](#_Toc146846443)

[Network Topology: 19](#_Toc146846444)

[IP Addressing Plan: 20](#_Toc146846445)

[Routing Protocol: 22](#_Toc146846446)

[i) FTP 22](#_Toc146846447)

[ii) SMTP 22](#_Toc146846448)

[iii) NTP 24](#_Toc146846449)

[iv) SSH(Local Login): 25](#_Toc146846450)

[v) AAA(tacacs+): 26](#_Toc146846451)

[vi) VLAN: 27](#_Toc146846452)

[viii) . NAT: 28](#_Toc146846453)

[Conclusion and future recommendation: 29](#_Toc146846454)

[Bibliography: 29](#_Toc146846455)

[Annex: 29](#_Toc146846456)

# 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, scalable 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 this project is to create an efficient and secure network Infrastructures which facilitates the doctor, nurses and other working staff of the hospital. Some of the key objective include:

1. **High speed internet connectivity.**
2. **Organized health records for future use.**
3. **Data Security and Privacy.**
4. **Efficient Data Sharing and Collaboration**

# Scope of the Project:

The scope of hospital network design surround various aspects related to the development, enhancement, and optimization of network infrastructure within healthcare facilities. The scope includes, but is not limited to, the following areas:

1. **Network Architecture**: Designing and implementing a network architecture that considers the specific requirements of hospitals. This involves planning the network topology, connectivity options, network segmentation, and scalability to accommodate future growth.
2. **Connectivity and Communication**: Ensuring reliable and high-speed connectivity within hospitals. This includes establishing robust wired and wireless networks to facilitate seamless communication between medical professionals, administrative staff, and patients. It will also help in maintaining Electronic Health Record.
3. **Network Security and Privacy**: Implementing security measures such as Asa firewall, Security policies etc to protect patient data, network infrastructure, and communication channels from unauthorized access, data breaches, and cyber threats.
4. **Telemedicine and Remote Patient Monitoring**: Enabling telemedicine services and remote patient monitoring through the network infrastructure. This involves establishing secure connections for video consultations, and real-time monitoring of patients in remote areas.

# Background Study and Literature Review:

This project is to design a state of the art network for a municipality 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

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. Here is the significance of the such design:

1. Hierarchical network design is commonly used in hospitals to ensure efficient data flow.
2. Star and mesh topologies offer redundancy and reliability benefits in hospital networks.
3. Network segmentation is vital to separate sensitive patient data from administrative systems.
4. Virtual LANs (VLANs) are utilized for efficient network management.
5. Patient data security is a top priority in hospital networks, necessitating robust encryption protocols.
6. Access control mechanisms and role-based access control (RBAC) are implemented to protect sensitive information.
7. Intrusion detection and prevention systems (IDPS) are used to detect and prevent network attacks.
8. Compliance with regulations like HIPAA and GDPR is crucial for healthcare data protection.
9. Hospital networks must be designed to accommodate future growth, including the addition of medical devices.
10. Scalable network architectures like spine-and-leaf are considered for data center networks.
11. Technologies like Network Function Virtualization (NFV) enable dynamic resource allocation.
12. Low latency is essential for real-time applications, such as telemedicine and remote surgery.
13. Quality of Service (QoS) mechanisms are used to prioritize critical medical traffic.
14. Load balancing techniques are employed to distribute network traffic evenly.
15. Redundancy in hardware and connections is crucial to ensure uninterrupted healthcare services.
16. Wi-Fi networks in hospitals require careful planning to guarantee coverage and capacity.
17. Wireless Medical Telemetry Service (WMTS) is used for monitoring medical devices.
18. Integration and security of IoT devices in the network are challenging due to their sheer number.
19. Isolation techniques are employed to separate IoT traffic from critical healthcare data.
20. Telemedicine applications depend on high-speed, reliable network connections.
21. Network design must prioritize telemedicine traffic to ensure quality service.
22. Balancing network performance and cost-effectiveness is a critical consideration in healthcare.
23. TCO (Total Cost of Ownership) analyses are conducted to assess network investments.

# Project Planning:

The project development began early in May of 2022. Firstly, all the major tasks related to the project and thesis writing were identified and listed. Then, , tasks were divided throughout the sprint. The divided task was completed within the allocated timeframe

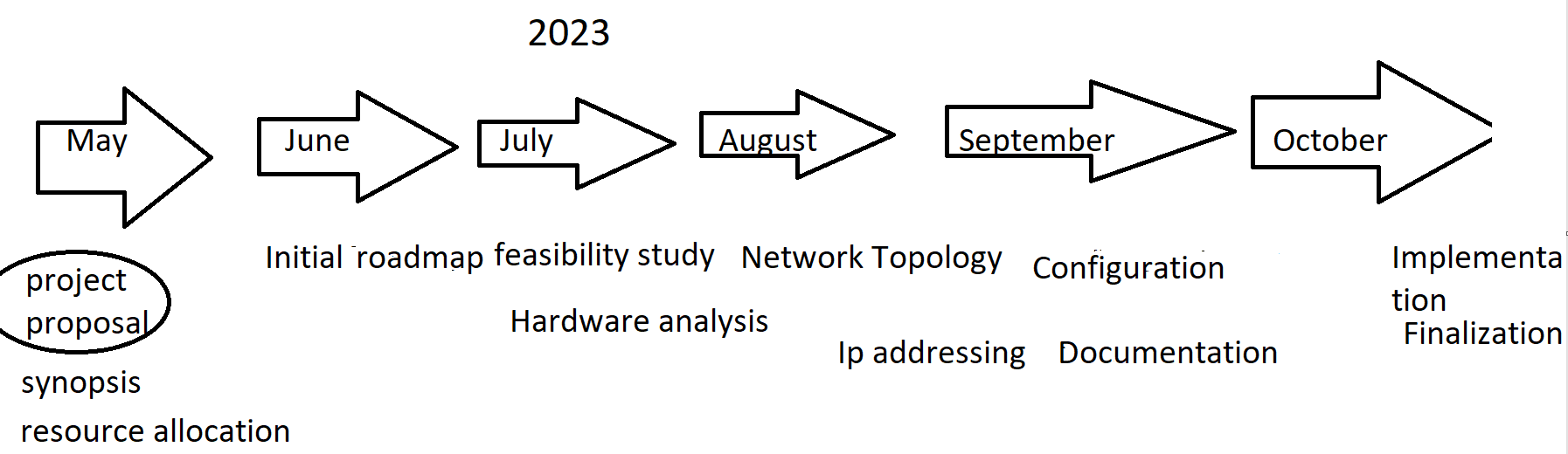


Fig : Timeline of Project

# Working Methodology:

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 our system:

* + 1. 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

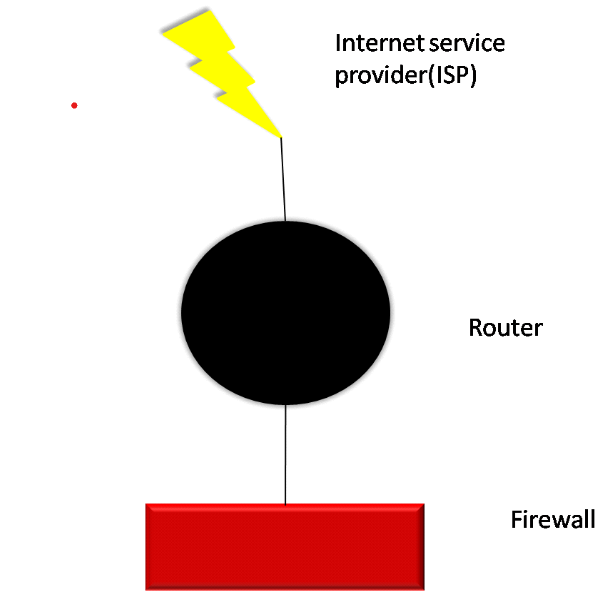
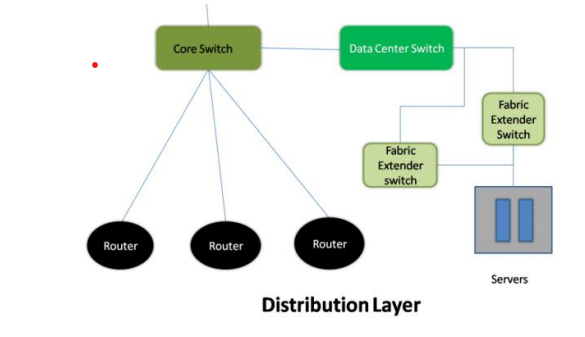
****

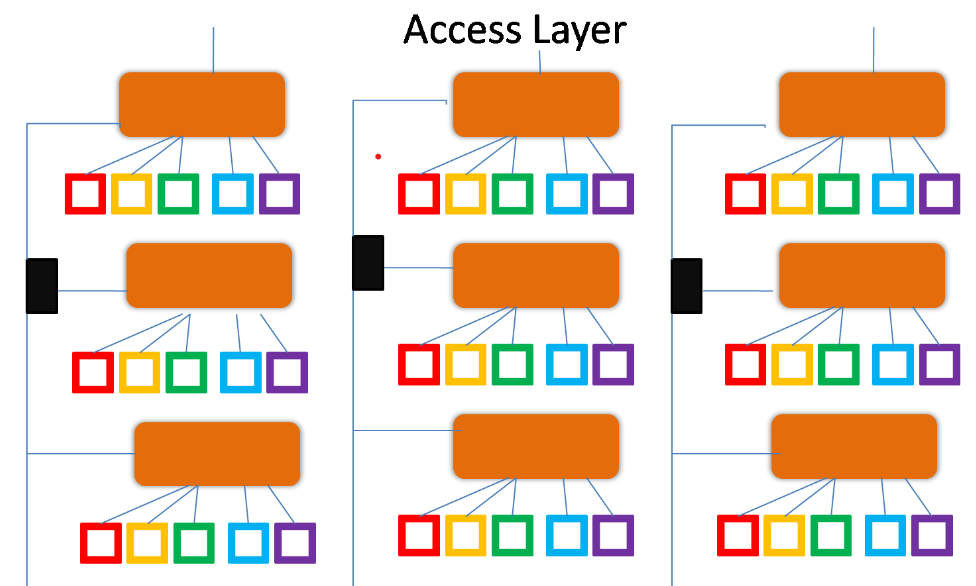
Fig: Core Layer Architecture

* + 1. DISTRIBUTION LAYER: The distribution layer is in charge of directing the packets. It additionally gives protocolbased 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.



**Fig: Distribution layer Architecture**

* + 1. 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.



Architecture of Access layer.

# 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. Design 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. Design the IP addressing scheme: The flat addressing scheme and static routes are not desirable features in a scalable growing network. So, hierarchical addressing is required.

c. Introduce a 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.

# 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 center 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, Fiber 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.

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:

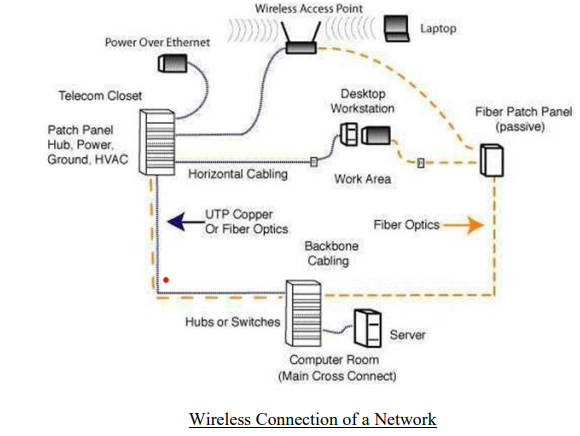
**•** Number of ports

. • 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.



# Implementation and Testing:

## 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

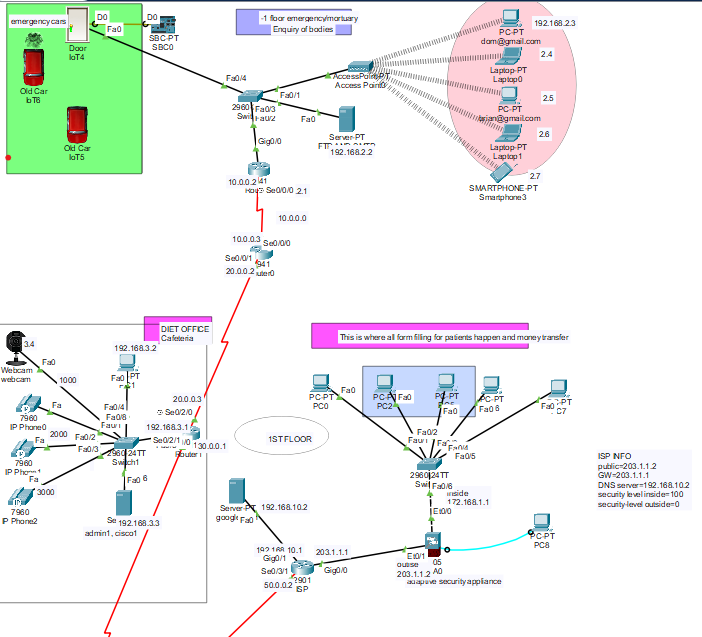
## Explanation of Distribution Layer (1st Floor):

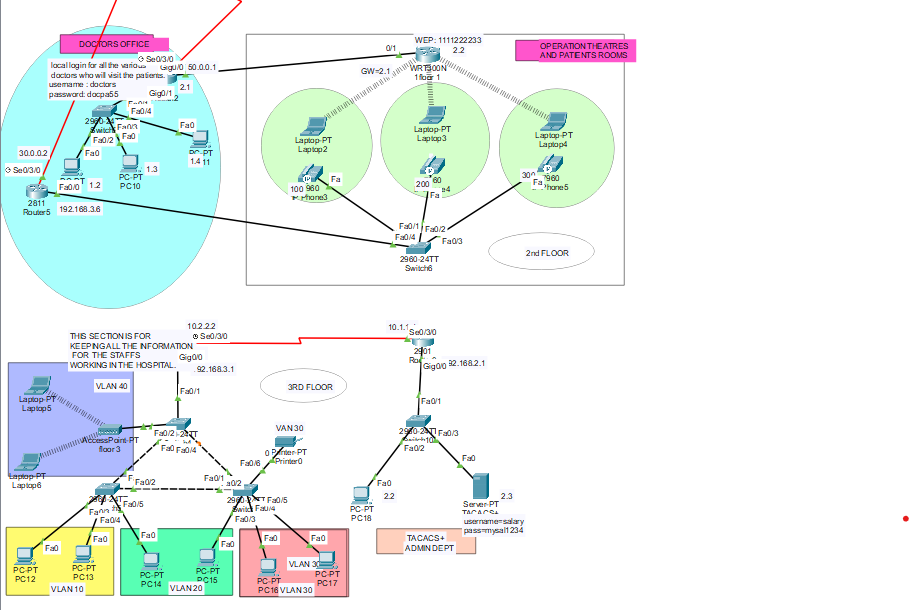
The area where the ASA firewall configured is implemented there because, that is the part of the hospital where people come and fill the forms and do the payment of money (if any operation/surgery is carried out). ASA is configured with NAT, DNS. It basically is the ISP. Waiting place for everyone will 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.

## 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 gives all the details to the first floor through the FTP or SMTP servers used devices making them aware who entered the emergency room and various kind of information’s.

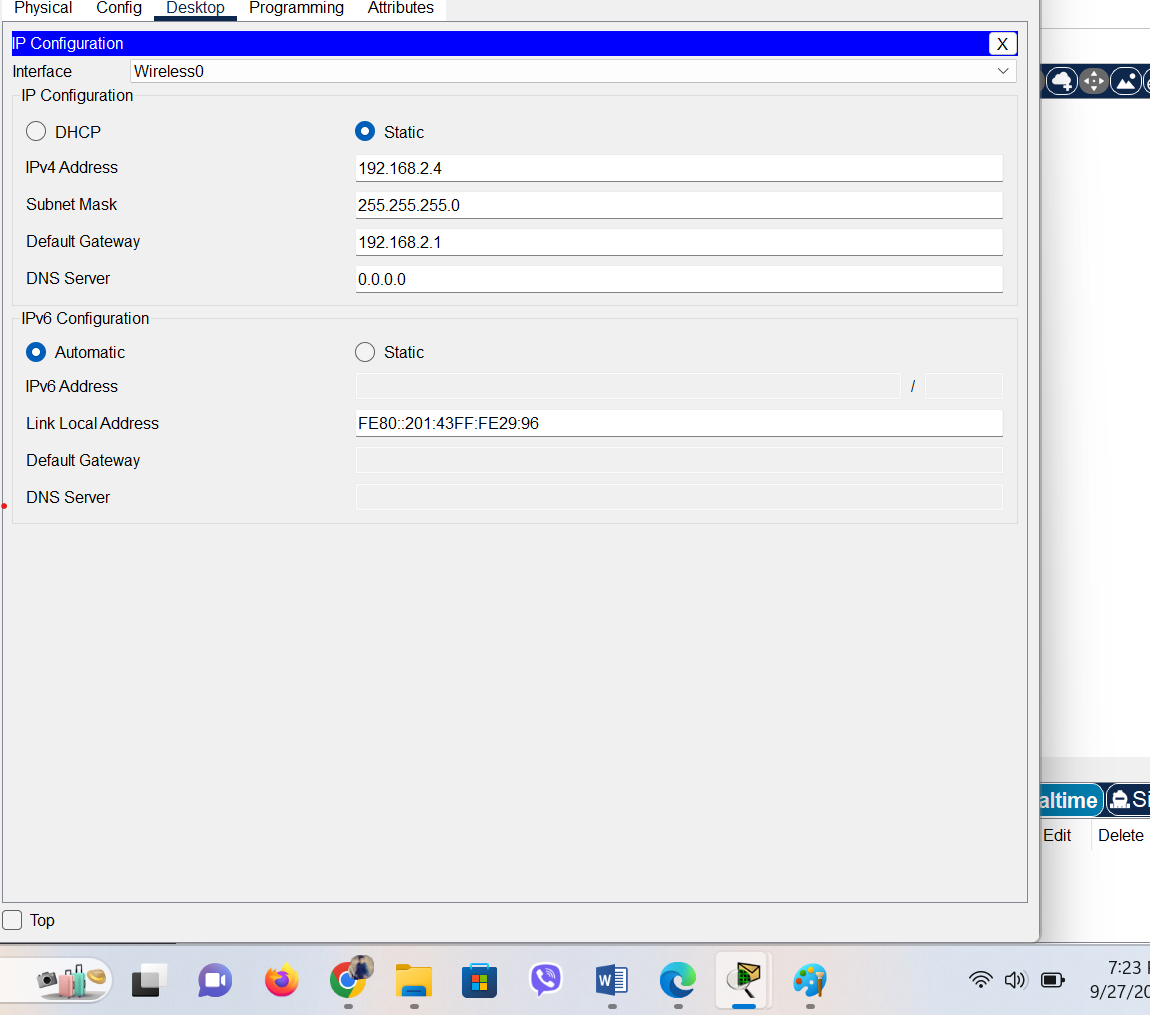
## Network Topology:





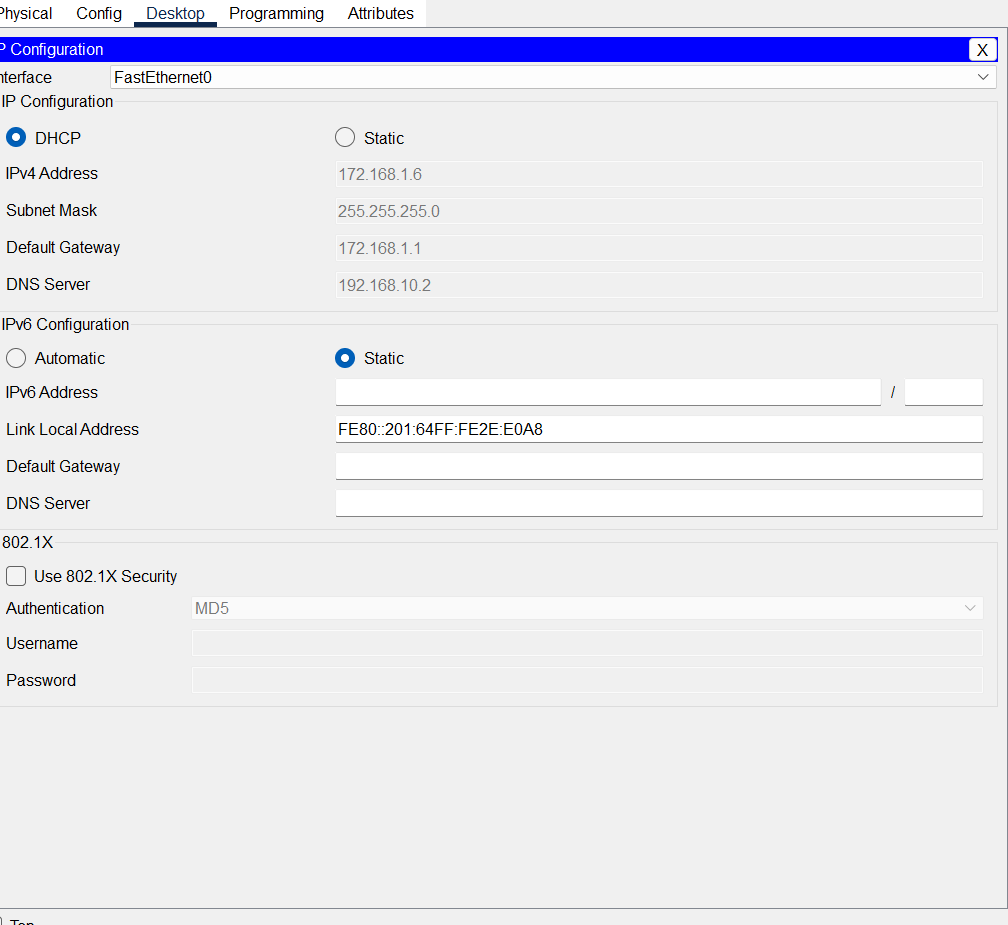
## IP Addressing Plan:

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.



Static Ip address

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.



## Routing Protocol:

In my Network I have used

1. FTP: FTP (File Transfer Protocol) is a [network protocol](https://www.techtarget.com/searchnetworking/definition/protocol) for transmitting files between computers over Transmission Control Protocol/Internet Protocol ([TCP/IP](https://www.techtarget.com/searchnetworking/definition/TCP-IP)) connections It is Used for file transferring between 2 different networks.
2. SMTP(Emails): SMTP stands for Simple Mail Transfer Protocol. It is a widely-used communication protocol for sending and receiving email messages on the internet. SMTP is part of the application layer of the TCP/IP protocol suite and is responsible for the transmission of email messages between email clients and email servers. It is Used for sending emails.

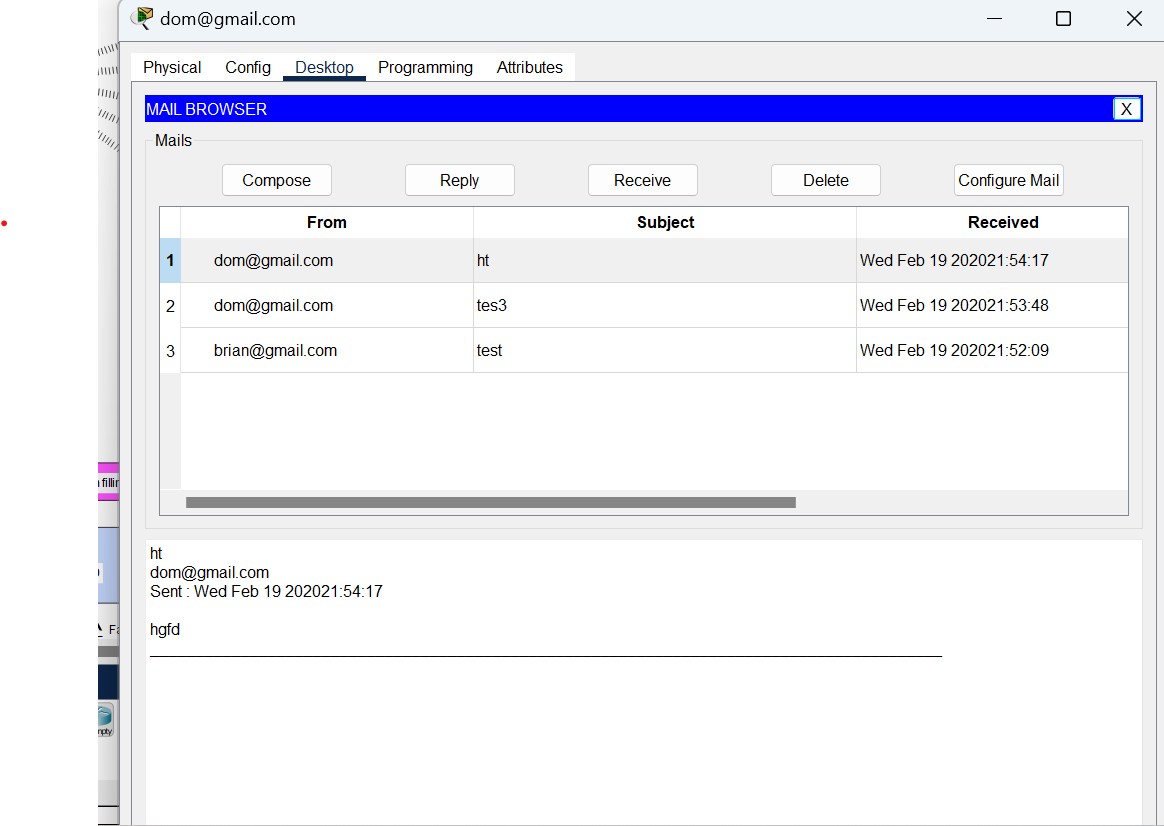


Fig-Smtp Verification

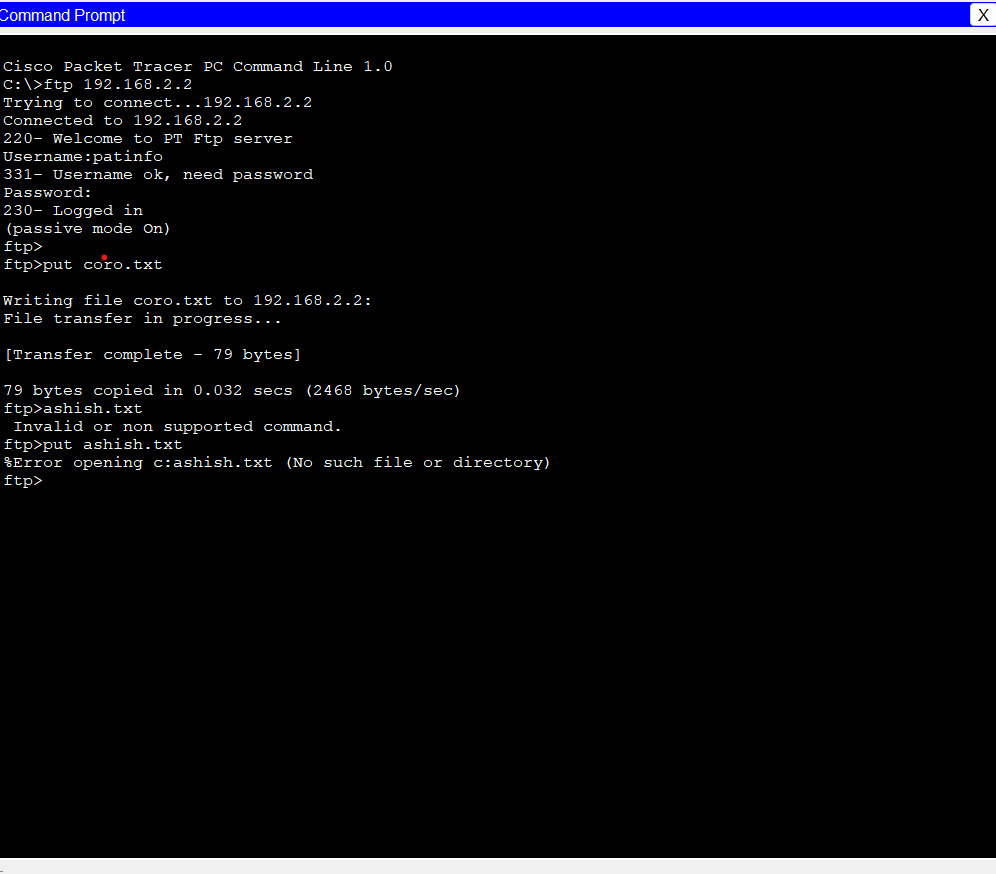


Fig: FTP verification

1. NTP: It is 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 .

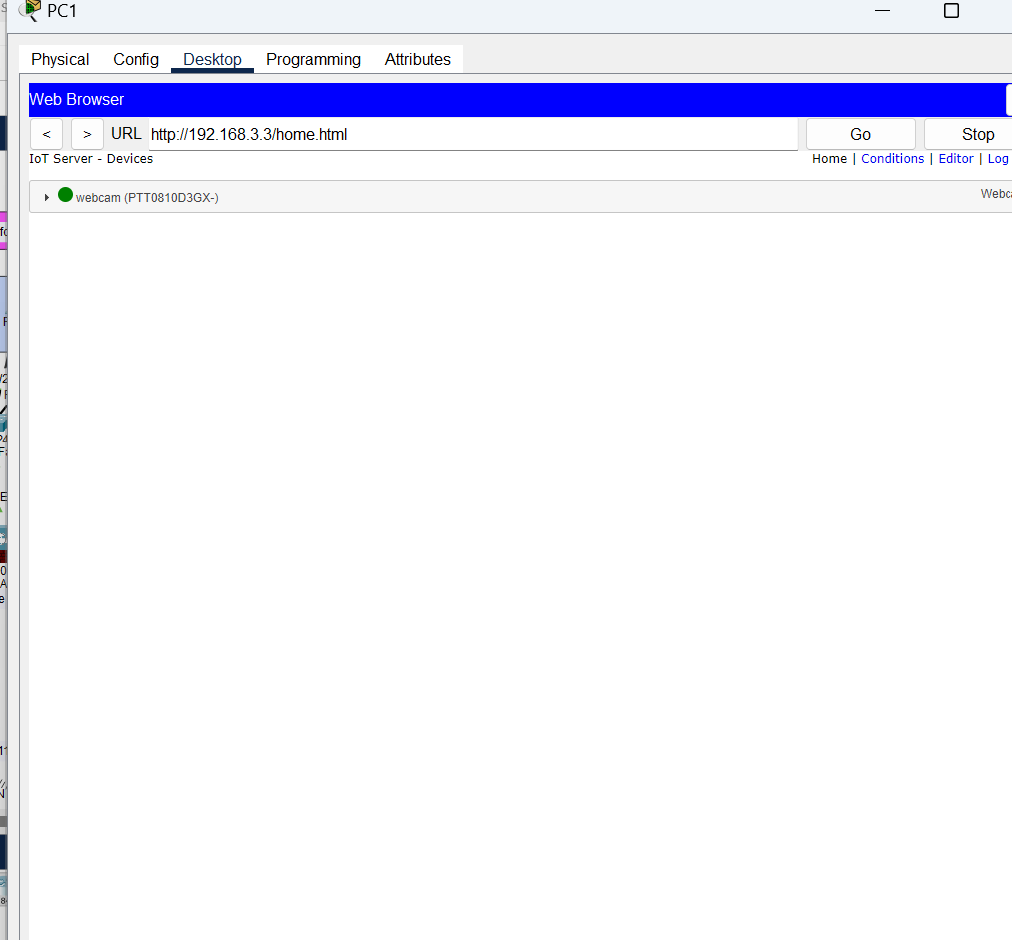
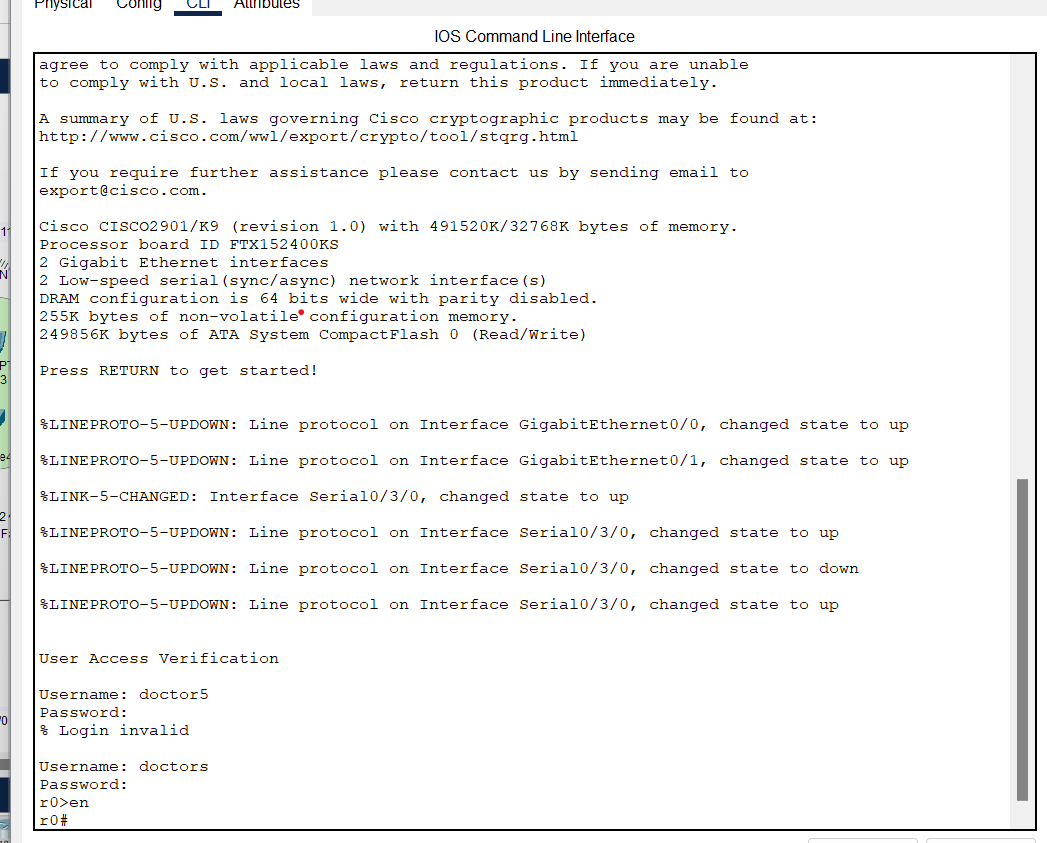


Fig: NTP verification

1. SSH(Local Login): It is Used so that for every doctor there is a separate username and password when the doctor enters his/her office. It makes the process reliable and convenient



SSH verification

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

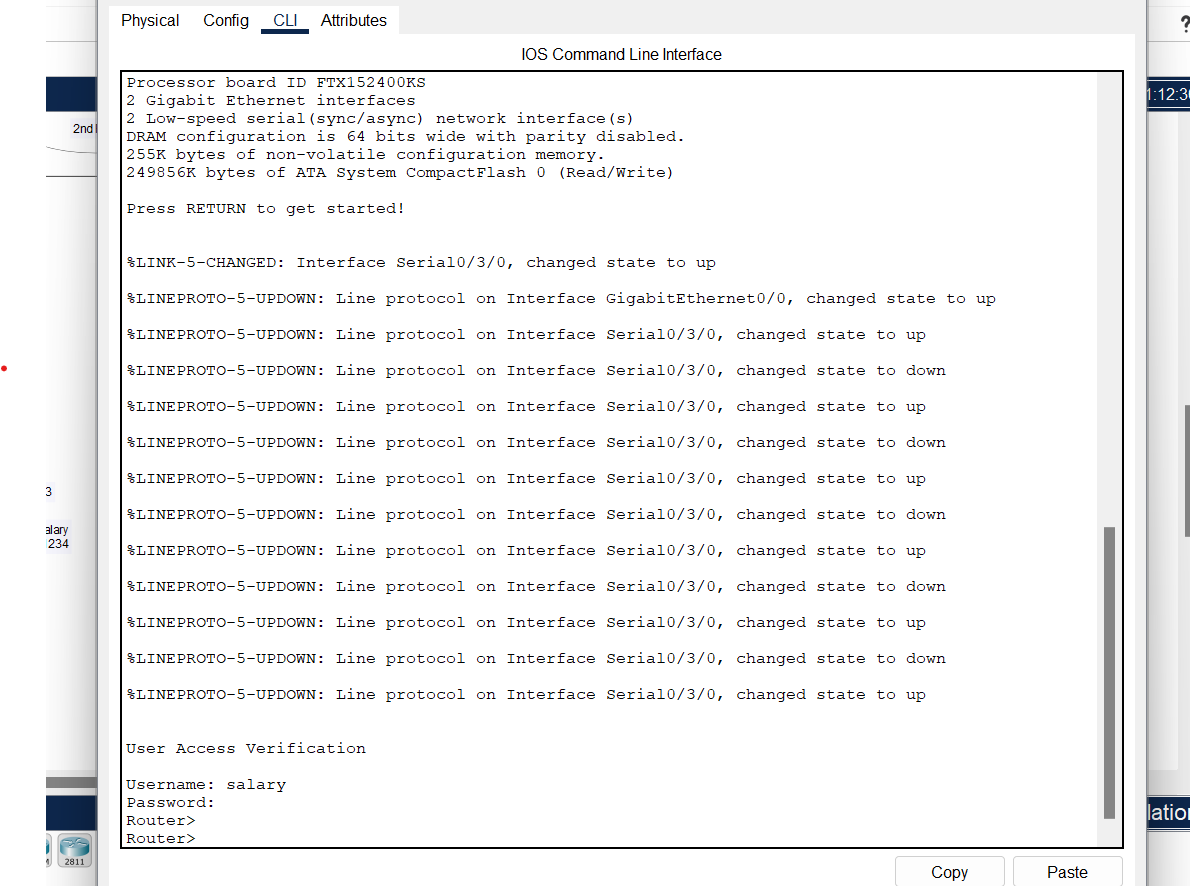
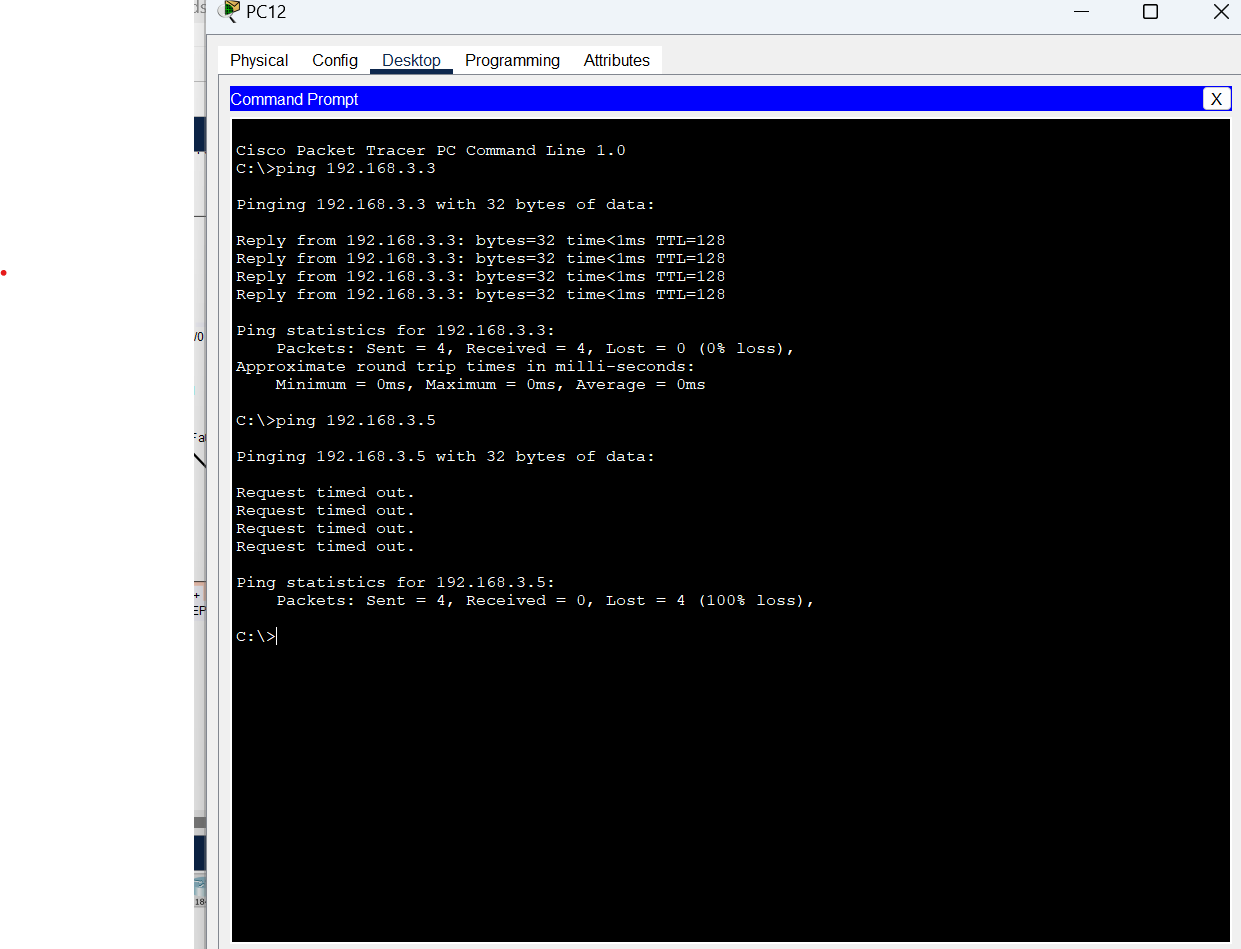


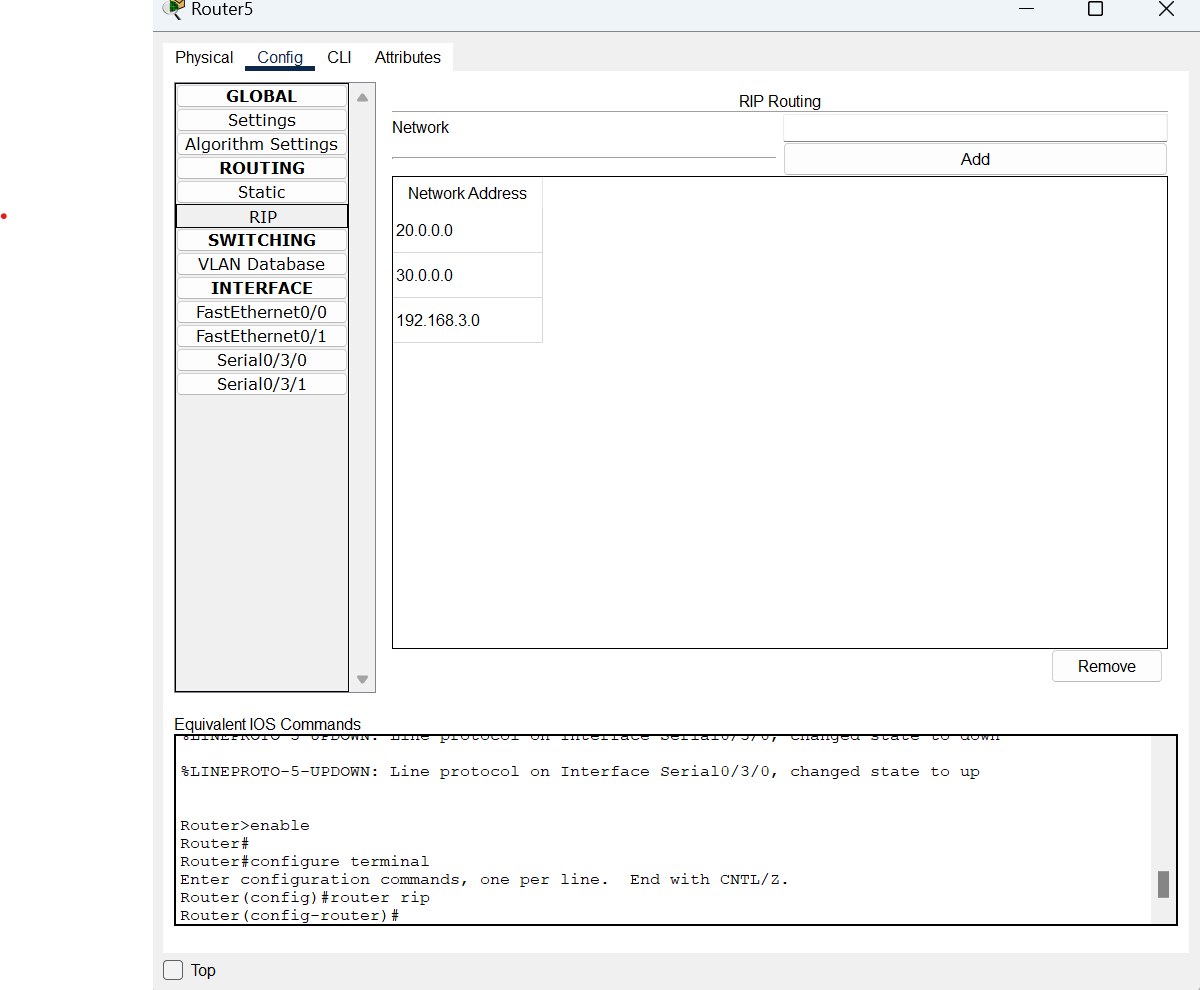
Fig: Tacacs+ verification

1. VLAN: . Virtual local area networks have become crucial for organizations with complex networking systems. Organizations require solutions that allows them to scale up their networks, segment them to increase security measures, and decrease network latency .Vlans are used for security internally among the same network.



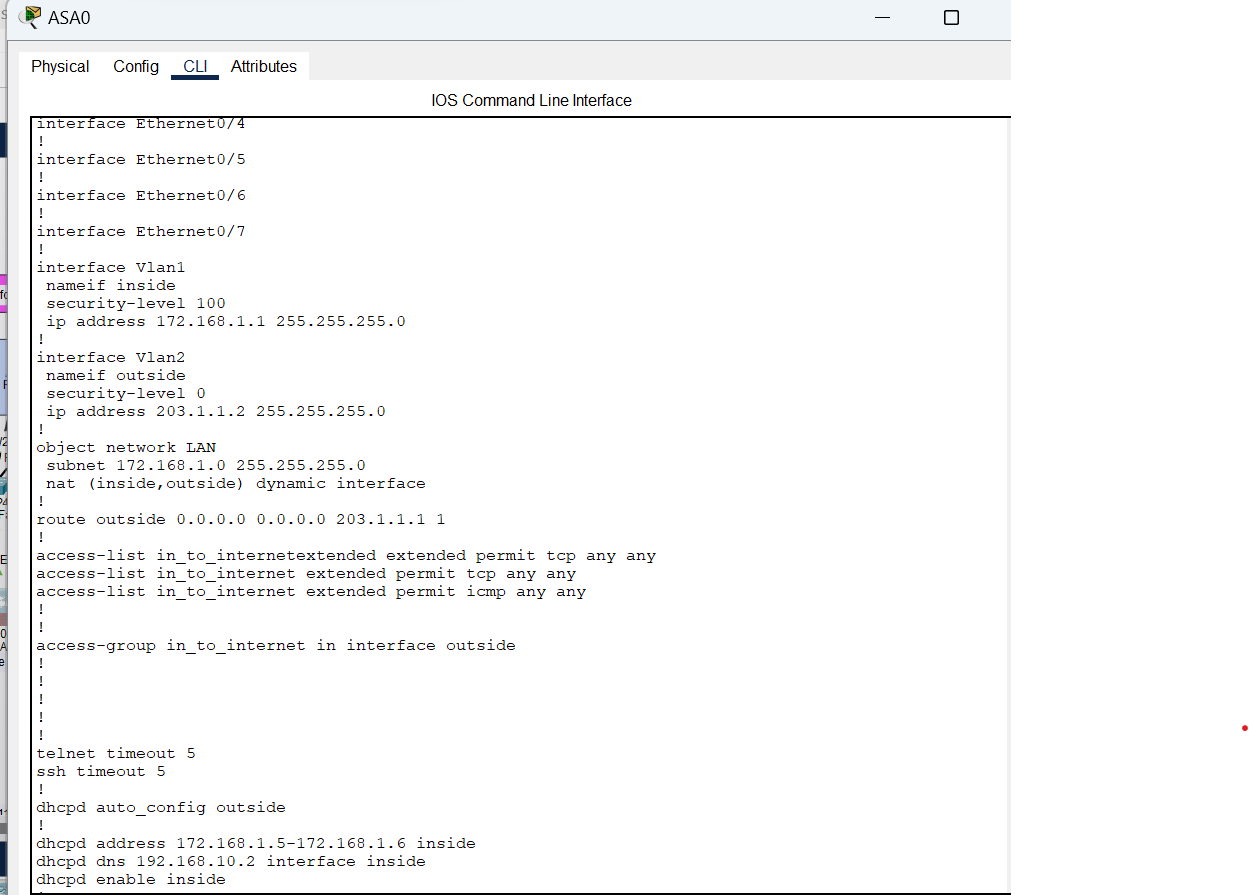
Ping from same vlan pc and 2nd from different vlan.

1. . RIP: It is routing protocol Used for communicating between 2 networks. It is based on distance vector or link state routing.



Rip Verification

1. . NAT: It is 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.



Verification of Nat configuration.

# Conclusion and future recommendation:

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

<https://epublications.regis.edu/cgi/viewcontent.cgi?article=1359&context=theses>

{3} <https://npbook.cs.purdue.edu/ixp1200/lnotes/490N.pdf>

# Annex:

Configuration of all Devices:

-**1 Floor emergency/mortuary**

**Router 4**

en

config t

#interface Serial0/0/0

#ip address 10.0.0.2 255.0.0.0

no sh

exit.

interface GigabitEthernet0/0

ip address 192.168.2.1 255.255.255.0

no sh

exit

router rip

network 10.0.0.0

network 20.0.0.0

network 192.168.2.0

network 192.168.3.0

**ServerPT**

ip address 192.168.2.2

FTP ans SMTP service

**Router 0**

interface Serial0/0/0

ip address 10.0.0.3 255.0.0.0

no sh

interface Serial0/0/1

ip address 20.0.0.2 255.0.0.0

no sh

router rip

network 10.0.0.0

network 20.0.0.0

network 192.168.2.0

**1st floor**

**Diet Office**

**Router 1**

en

config t

interface FastEthernet0/0

ip address 192.168.3.1 255.255.255.0

no sh

exit

interface Serial0/2/0

ip address 20.0.0.3 255.0.0.0

no sh

exit

interface Serial0/2/1

ip address 30.0.0.1 255.0.0.0

no sh

exit

router rip

network 10.0.0.0

network 20.0.0.0

network 192.168.2.0

network 192.168.3.0

exit

ip dhcp pool pool1

network 192.168.3.0 255.255.255.0

default-router 192.168.3.1

ip dhcp excluded-address 192.168.3.1 192.168.3.6

Ip phone 0

number:1000

Ip phone 1

number:2000

Ip phone 2

number:3000

**webcam**

ip:192.168.3.4/24

remote server:192.168.3.3

**Server**

ip address:192.168.3.3

IOT service enabled

Username:admin1

Password:cisco1

**Form Filling and Money Transfer**

**Isp router**

en

config t

interface GigabitEthernet0/0

ip address 203.1.1.1 255.255.255.0

no sh

exit

interface GigabitEthernet0/1

ip address 192.168.10.1 255.255.255.0

no sh

exit

interface Serial0/3/1

ip address 50.0.0.2 255.0.0.0

no sh

exit

router rip

network 30.0.0.0

network 50.0.0.0

network 192.168.2.0

network 192.168.10.0

network 192.178.1.0

network 203.1.1.0

**ASA firewall:**

interface Vlan1

nameif inside

security-level 100

ip address 172.168.1.1 255.255.255.0

interface Vlan2

nameif outside

security-level 0

ip address 203.1.1.2 255.255.255.0

object network LAN

subnet 172.168.1.0 255.255.255.0

nat (inside,outside) dynamic interface

route outside 0.0.0.0 0.0.0.0 203.1.1.1 1

Access control

access-list in\_to\_internetextended extended permit tcp any any

access-list in\_to\_internet extended permit tcp any any

access-list in\_to\_internet extended permit icmp any any

access-group in\_to\_internet in interface outside

dhcpd auto\_config outside

dhcpd address 172.168.1.5-172.168.1.6 inside

dhcpd dns 192.168.10.2 interface inside

dhcpd enable inside

**Server pt**

ip address:192.168.10.2

Dns Service enabled

**Doctor Office**

Router r0

en

config t

aaa new-model

aaa authentication

aaa authentication login default local

username doctors

privilege 15 password docpa55

line vty 0 4

login authentication SSH-LOGIN

transport input ssh

interface GigabitEthernet0/0

ip address 192.168.2.1 255.255.255.0

no sh

exit

interface GigabitEthernet0/1

ip address 192.168.1.1 255.255.255.0

no sh

exit

interface Serial0/3/0

ip address 50.0.0.1 255.0.0.0

no sh

router rip

network 30.0.0.0

network 50.0.0.0

network 172.168.0.0

network 192.168.1.0

network 192.168.2.0

network 192.168.10.0

**Router 5**

ip dhcp excluded-address 192.168.3.1 192.168.3.10

ip dhcp pool phone

network 192.168.3.0 255.255.255.0

default-router 192.168.3.6

option 150 ip 192.168.3.6

interface FastEthernet0/0

ip address 192.168.3.6 255.255.255.0

interface Serial0/3/0

ip address 30.0.0.2 255.0.0.0

router rip

network 20.0.0.0

network 30.0.0.0

network 192.168.3.0

dial-peer voice 1 voip

destination-pattern 1000...

session target ipv4:192.168.3.1

telephony-service

max-ephones 3

max-dn 3

ip source-address 192.168.3.6 port 2001

auto assign 1 to 5

ephone-dn 1

number 100

ephone-dn 2

number 200

ephone-dn 3

number 300

**Operation Theatre and Pateint Room**

**WEP**

key:111122223333

**Admin Section(3rd floor)**

**Router 3**

interface GigabitEthernet0/0

ip address 192.168.3.1 255.255.255.0

interface Serial0/3/0

ip address 10.2.2.2 255.255.255.0

router rip

network 10.0.0.0

network 192.168.2.0

network 192.168.3.0

**Router 8**

interface GigabitEthernet0/0

ip address 192.168.2.1 255.255.255.0

interface Serial0/3/0

ip address 10.1.1.1 255.255.255.0

router rip

network 10.0.0.0

network 192.168.2.0

network 192.168.3.0

aaa new-model

aaa authentication login default group tacacs+ local

username salary

privelage 14 password:mysal1234

tacacs-server host 192.168.2.3

tacacs-server key tacacspa55

**Server**

client name:main hub

ip address:192.168.2.1

secret key:tacacspa55

server type:Tacacs

**Switch4:**

interface FastEthernet0/2

switchport access vlan 40

switchport mode access

**Switch 5**

interface FastEthernet0/3

switchport access vlan 10

switchport mode access

interface FastEthernet0/4

switchport access vlan 10

switchport mode access

interface FastEthernet0/5

switchport access vlan 20

switchport mode access

**Switch 7**

interface FastEthernet0/3

switchport access vlan 20

switchport mode access

interface FastEthernet0/4

switchport access vlan 30

switchport mode access

interface FastEthernet0/5

switchport access vlan 30

switchport mode access

interface FastEthernet0/6

switchport access vlan 30

switchport mode access