A Mini Project Report on

Hospital Management System using Cisco Packet Tracer

Submitted in partial fulfilment of the requirements
Of the Semester VII Subject of

Network Design Lab

in

Information Technology

by

Vipul Karle	**Roll no:- 27**
Samidha vele	**Roll no :- 74**
Mrunali Virkud	**Roll no :- 75**
Anket Uppal	**Roll no :- 72**

Subject Incharge

Prof. V. M. Kharche

Konkan Gyanpeeth College Of Engineering, Karjat 410201

University Of Mumbai

2021-2022

CERTIFICATE

This is to certify that Network Design Lab (NDL) Mini Project entitled Hospital Management System using Cisco Packet Tracer Submitted by Vipul Karle (Roll no.27), Samidha Vele (Roll no. 74), Mrunali Virkud (Roll no. 75), Anket Uppal (Roll no.72) for the partial fulfilment 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 2021-2022

Prof. V. M. Kharche
Subject Incharge

Prof.
Head of Department

Declaration

We Declare that this written submission represents our ideas in our own words and where others ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we 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. We 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 of Students

Vipul Karle()

Samidha Vele(75)

Mrunali Virkud(74)

Anket Uppal(72)

Acknowledgements

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 **Prof** 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.

Content:

1.Introduction

Now more than ever, excellent patient care relies on staff having the tools to access the most up-to-date information to enhance the clinical decision-making process. When the nurses talk about charting, they are usually referring to the thorough, timely documentation of the patient's status based on their nursing assessments, and the interventions they perform based on their vital signs, lab data, and more. They also chart about medication administration, and their observations of the patient's response to the therapy. It is no secret that networking has become an essential part of our lives. Once the new reporting environment is integrated into the network, users will be able to build reports by selecting the criteria, measures, and output formats that are specific to the patient's needs. Hospital / Health Network will be able to eliminate the data islands across the organization, simplify how information is distributed among users, and increase employee efficiency. Users will also be able to obtain information from the entire network, eliminating the need to manually locate, collate, and analyze the data. With these reporting tools in the hands of clinicians, the business will be able to ensure that information is standardized across the network.

2.Objectives

Main objectives of a Hospital Management System are:

- Design a system for better patient care.
- Reduce hospital operating costs.
- Provide MIS (Management Information System) report on demand to management for better decision making.
- Better co-ordination among the different departments.
- Provide top management a single point of control.
- Hospital management System handles activities of major departments in a hospital like:
  1. Front Office/OPD Management
  2. Patient management (scheduling, registration and long-term care)
  3. Patient care management and departmental modules (radiology, pharmacy and pathology labs)
  4. Investigative Labs
  5. Billing
  6. Medical Stores
  7. Financial Accounting (billing, insurance processing, materials management, accounts payable/receivable, payroll and general ledger)
  8. Payroll
- Hospital management system can be developed by using waterfall model which is a popular version of development life cycle model for software engineering. It describes a development method that is linear and sequential. It has distinct goals for each phase of development. In this model once, a phase of development is completed, there is no turning back, the development proceeds to the next phase. The advantage of this model is that it allows for departmentalization and managerial control.

3. Network Requirements

In Health care Network topology, we have desktop Computer, laptops, smart phone. There is a data flow between the devices within the system. We have divided our network into segments like for Hospital wards, clinical area etc. We have also used SSH for security. Our network requirements include network devices like routers, switches, server.

4. Major Design Areas And Functional Areas

The Functional Areas are:

Registration Process of SRS (Software Requirements Specification)

● Adding Patients: The Hospital Management enables the staff in the front desk to include new patients to the system.

● Assigning an ID to the patients: The HMS enables the staff in the front desk to provide a unique ID for each patient and then add them to the record sheet of the patient. The patients can utilize the ID throughout their hospital stay.

Check Out of SRS:

● Deleting Patient ID: The staff in the administration section of the ward can delete the patient ID from the system when the patient's checkout from the hospital.

● Adding to beds available list: The Staff in the administration section of the ward can put the bed empty in the list of beds-available.

Report Generation of SRS:

● Information of the Patient: The Hospital Management System generates a report on every patient regarding various information like patients name, Phone number, bed number, the doctor's name whom its assigns, ward name, and more.

● Availability of the Bed: The Hospital Management system also helps in generating reports on the availability of the bed regarding the information like bed number unoccupied or occupied, ward name, and more.

Database of SRS:

● Mandatory Patient Information: Every patient has some necessary data like phone number, their first and last name, personal health number, postal code, country, address, city, 'patient's ID number, etc.

● Updating information of the Patient: The hospital management system enables users to update the information of the patient as described in the mandatory information included.

5. Existing Infrastructure

Hospital management system is a computer system that helps manage the information related to health care and aids in the job completion of health care providers effectively. They manage the data related to all departments of healthcare such as,

- Clinical
- Financial
- Laboratory
- Inpatient
- Outpatient
- Operation theater
- Materials
- Nursing
- Pharmaceutical
- Radiology
- Pathology etc.

6. Network Devices

In networking, a hierarchical design is used to group devices into multiple networks. The networks are organized in a layered approach. The hierarchical design model has three basic layers:
Core layer: Connects distribution layer devices
Distribution layer: Interconnects the smaller local networks
Access layer: Provides connectivity for network hosts and end devices

Routers

A router is a physical network device (usually running proprietary software) that is used to connect several network segments into one network or an existing large network into smaller subnets. Routers operate on the Network layer 3 of the OSI model and unite multiple physical network segments into a single seamless, logical network by understanding how to forward traffic from a sender to ultimately reach an intended receiver. This means that routing behavior is influenced strongly by the protocols in use. To some extent, therefore, understanding routing also requires understanding how Network layer protocols behave. A router directs a packet to its network or Internet destination using routing protocols to exchange information and determine routing decisions. Routing exists in an intranet between routing devices and on the ISP network between a border gateway router and a router.

Routers maintain routing tables that are consulted every time a packet needs to be redirected from one interface or segment to another. Routes can be added manually to the routing table—a very secure but less-manageable method, depending on the size of the network—or be updated automatically using routing protocols such as the following:

- Routing Information Protocol (RIP)/RIPv2

- Interior Gateway Routing Protocol (IGRP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPF), Border Gateway Protocol (BGP)
- Exterior Gateway Protocol (EGP)
- Intermediate System-Intermediate System (IS-IS)

Routing protocols employ different techniques to prevent routing loops (when a packet is rerouted indefinitely without finding the destination). Some of these techniques are:

- Counting to infinity
- Route poisoning
- Split horizon

Knowing how the routing protocols work is extremely important in avoiding trouble situations, such as:

- A hacker sending a route update to your network and poisoning (marking as downed) an important route to cause a DoS condition
- The creation of a routing loop that overloads the router and causes the network to become very slow and appear over- utilized\The update of a route to send all outbound traffic to a different host, which would then forward it to the ISP, launching an active interception or man-in-the- middle attack.

Switches

Switches, as in Figure are a special type of hub that offers an additional layer of intelligence to basic, physical-layer repeater hubs. A switch must be able to read the MAC address of each frame it receives. This information allows switches to repeat incoming data frames only to the computer or computers to which a frame is addressed. This speeds up the network and reduces congestion. Switches operate at both the physical layer and the data link layer of the OSI Model.

Fig. The Interface of a Switch with Ports

7. Request For Proposal (RFP)

A request for proposal (RFP) is an official document that announces and outlines plans for a specific project that any hospital or other healthcare facility plans to undertake. The purpose of issuing a formal request for proposal is to solicit bids from qualified contractors and suppliers to complete the proposed project.

Most requests will contain a detailed description of the project—including goals, timeline, budget, and technical requirements—in addition to providing background information about the company's mission and objectives. RFPs will also contain a section with guidelines for contractors and suppliers submitting a proposal in response to the project.

Requests for proposal can be used to procure a wide variety of different services. In healthcare, a hospital might issue an RFP for any of the following reasons:

- To expand or renovate a facility
- To implement a new technology
- To install durable medical equipment
- To solicit new food management services
- To request facility maintenance, repair, or inspection
- To secure emergency or non-emergency transportation services

Once contractors and suppliers have submitted their proposals, the issuing company will enter into negotiations with the most qualified applicants until one project bid is selected.

8. Remote Site Connectivity

Remote support can be implemented as an integrated par of a computer-based system in which dedicated software is return as a part of the system application. Such solutions will often be used for very sophisticated devices offering e.g. constant monitoring of the system.
Alternatively, a remote support is implemented with third party software solutions such as NetOp from Danware or pcAnywhere from Symantec.
Both NetOp and pcAnywhere consist of two application – a host application and a guest application. The host application is installed on computer system, which should be accessed remote, and the guest application is the program used to access the host.
A communication between the host and the guest can be either point – to point a communication using a modem connection between two stations (FIG.1) or a network connection using the internet (FIG.2).

FIG. 1

FIG. 2

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.

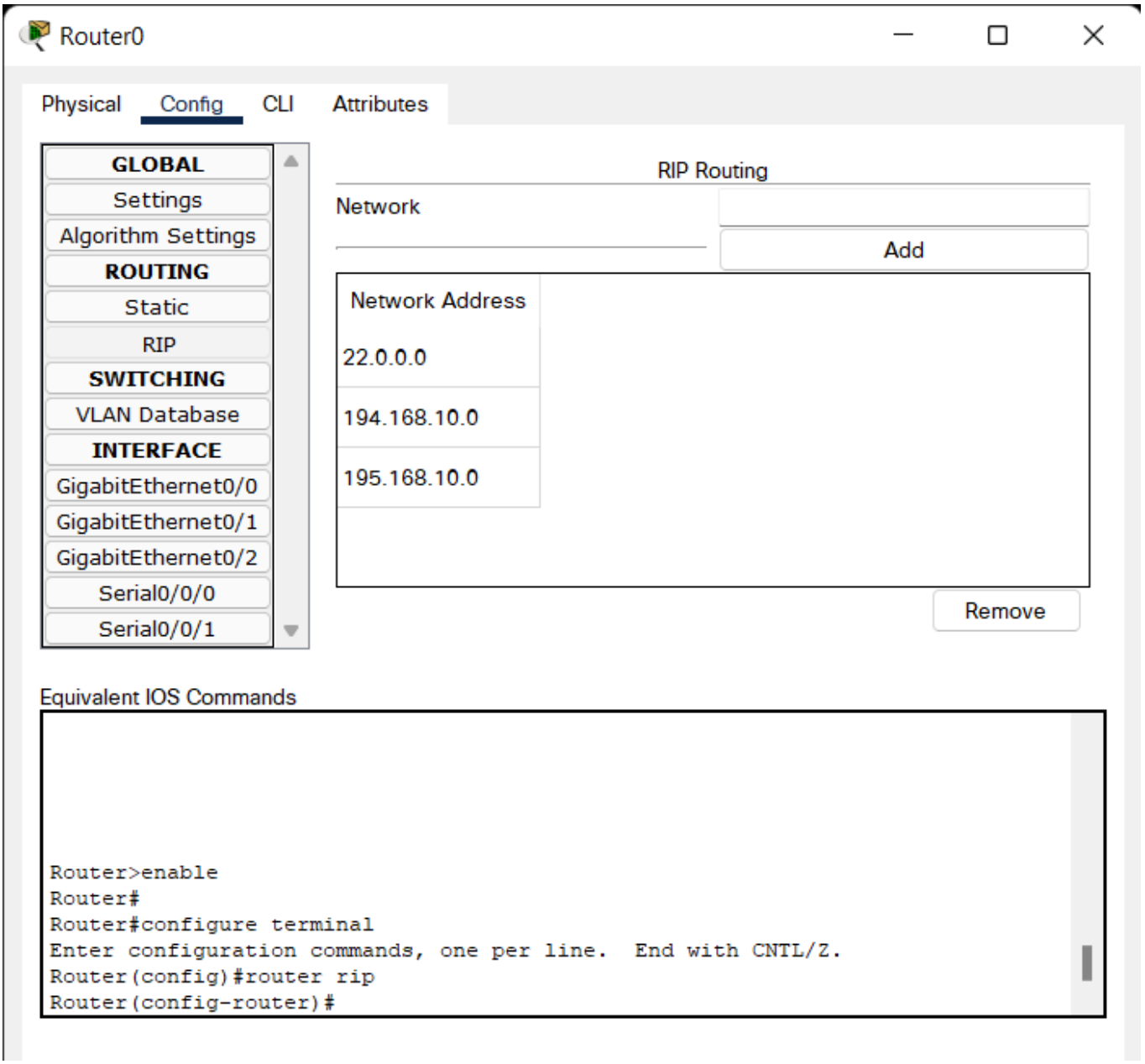

Fig. Configuration of RIP

9. IP Addressing Plan

An IP (Internet Protocol) address is a unique identifier for a node or host connection on an IP network. An IP address is a 32 bit binary number usually represented as 4 decimal values, each representing 8 bits, in the range 0 to 255 (known as octets) separated by decimal points. This is known as "dotted decimal" notation. Every IP address consists of two parts, one identifying the network and one identifying the node. The Class of the address and the subnet mask determine which part belongs to the network address and which part belongs to the node address.

There are 5 different address classes. One can determine which class any IP address is in by examining the first 4 bits of the IP address as follows:

Class A addresses begin with 0xxx, or 1 to 126 decimal.

Class B addresses begin with 10xx, or 128 to 191

decimal. Class C addresses begin with 110x, or 192 to

223 decimal. Class D addresses begin with 1110, or 224

to 239 decimal. Class E addresses begin with 1111, or

240 to 254 decimal.

Subnet Masking

Applying a subnet mask to an IP address allows you to identify the network and node parts of the address. The network bits are represented by the 1s in the mask, and the node bits are represented by the 0s.

Performing a bitwise logical AND operation between the IP address and the subnet mask results in the Network Address or Number.

Default subnet masks

The following are the default subnet masks:

Class A - 255.0.0.0 - 11111111.00000000.00000000.00000000

Class B - 255.255.0.0 - 11111111.11111111.00000000.00000000

Class C - 255.255.255.0 - 11111111.11111111.11111111.00000000

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.

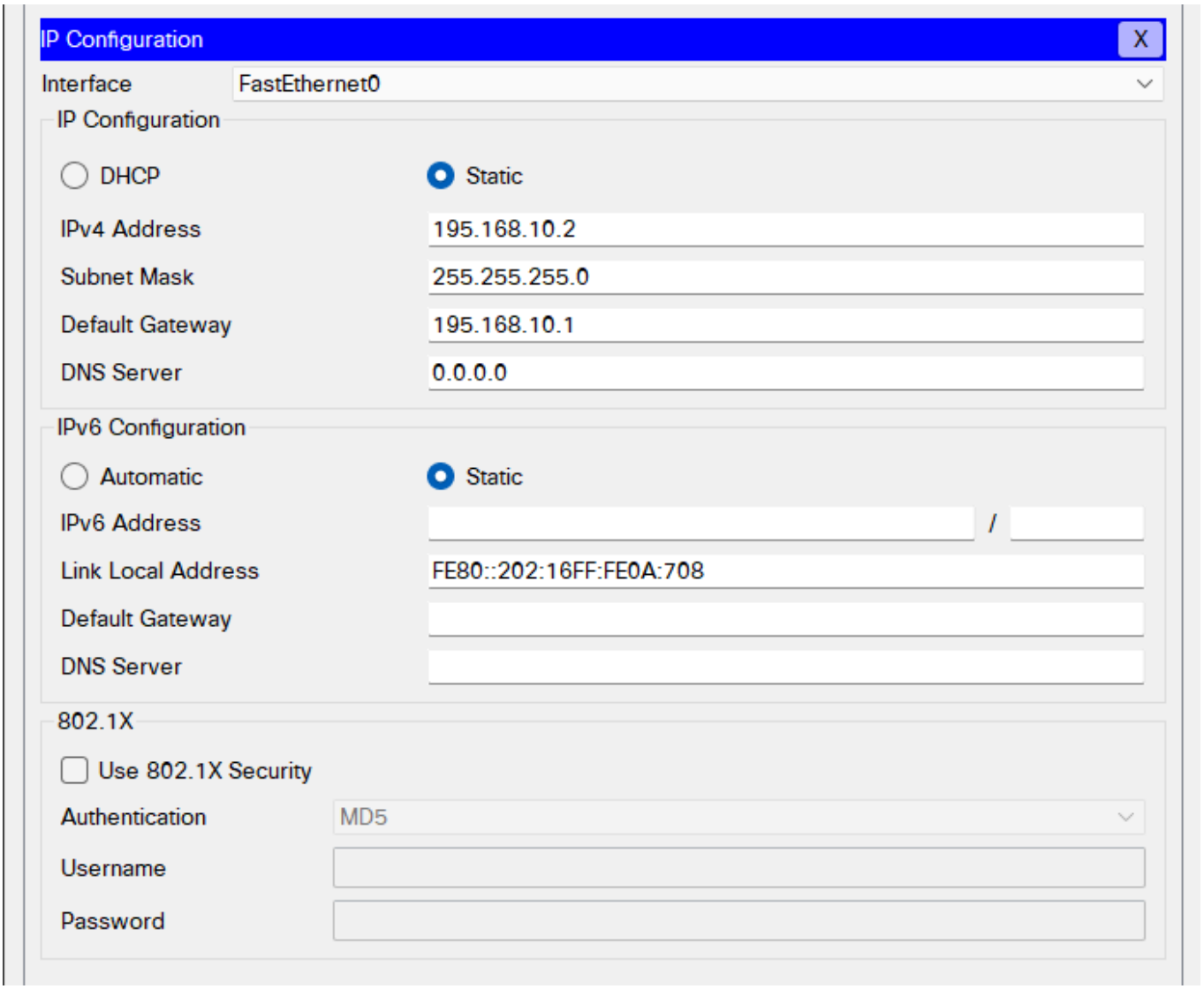

Fig. Static IP Addressing

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.

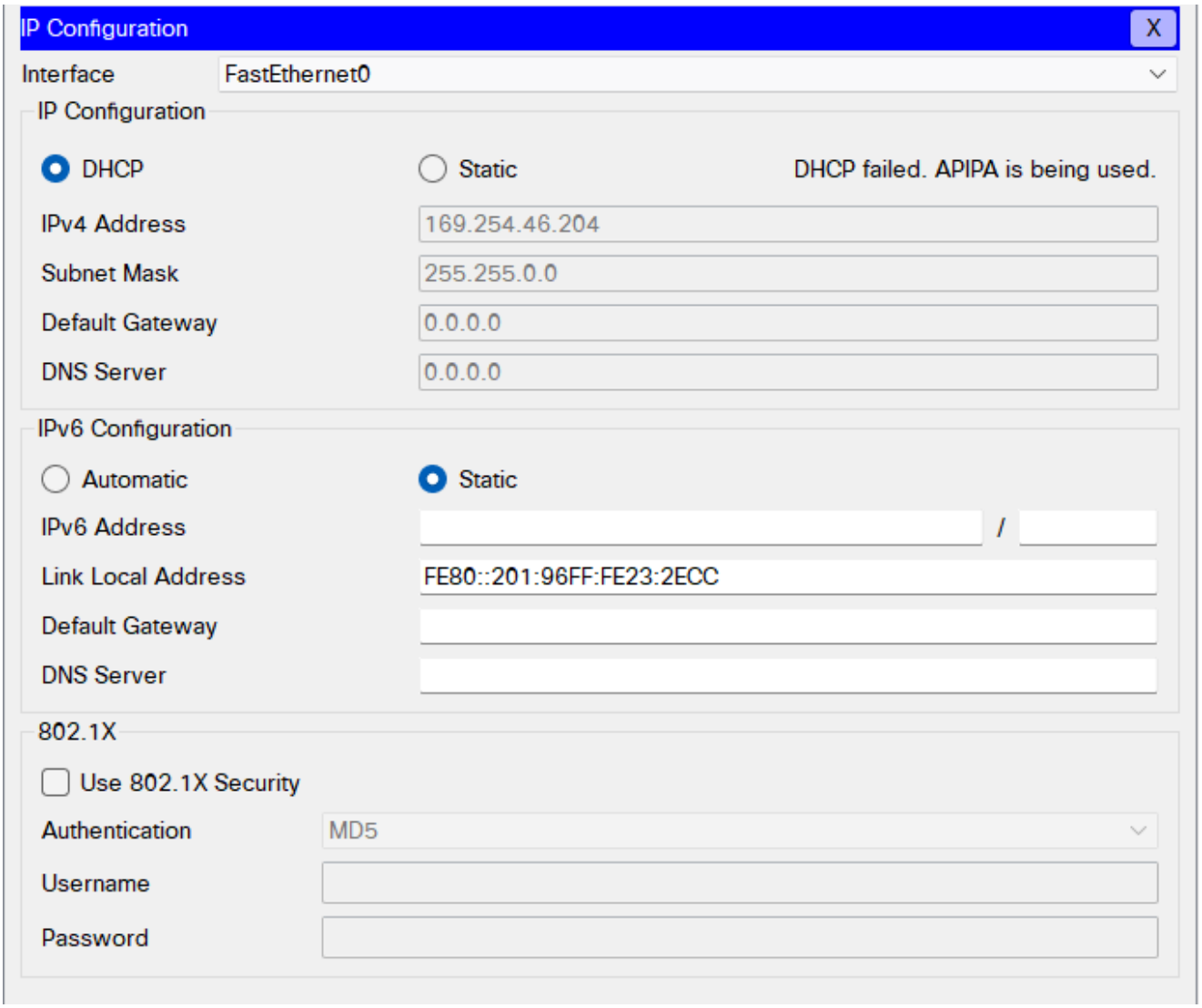

Fig. DHCP IP Addressing

10. Routing Protocol Plan

Routing is the process of moving packets from one network to another. The routing decision takes place at the source network device. That is a router. The decision is made based on metrics used for a particular routing protocol. Routing protocols may use some or all of the following metrics in determining the best route to a destination network:

a. Path length
b. Reliability
c. Delay
d. Bandwidth
e. Load
f. Communication cost

Path length is measure in either a cost or a hop count. In link-state routing protocols, the cost is the sum of the costs associated with each link in the path. Distance-vector routing protocols assign a hop count to the path length, which measures the number of routers a packet traverses between the source and destination.

Reliability is typically the bit-error rate of a link connecting this router to a source or destination resource. For most of the routing protocols, the reliability of a link is assigned by the network engineer. Since it is arbitrary it can be used to influence and create paths that are favorable over other paths.

The delay metric is an overall measurement of the time it takes for a packet to move through all the internetworked devices, links and queues of each router. In addition, network congestion and the overall distance traveled between the source and destination are taken into consideration in evaluating the delay metric value. Because the delay value takes into account many different variables, it is an influential metric on the optimal path calculation.

Using bandwidth as a metric in optimal path calculations may be misleading. Though bandwidth of a bandwidth of 1.54 Mbps is greater than 56 Kbps, it may not be optimal due to the current utilization of the link or the load on the device on the receiving end of the link.

The load is a metric that assigns a value to a network resource based on the resources overall utilization. This value is a composite of CPU utilization, packets processed per second, and disassembly/reassembly of packets among other things. The monitoring of the device resources itself is an intensive process.

In some cases, communication lines are charged based on usage versus a flat monthly fee for public networks. For example, ISDN lines are charged based on usage time and potential the amount of data transmitted during that time. In these instances, communication cost becomes an important factor in determining the optimal route.

11. Network Design(Topology Created)

The diagram is properly commented. Hospital Segments representing different departments of hospital. We have mentioned the IP addresses on each and every interface of the hosts and routers. The network was designed using different technologies which were very important and crucial for the completion of the task at hand. These technologies deployed were:

a) The Network Architecture

b) Network Connectivity

c) Ping Test

Network Architecture

The network architecture of Hospital management System network generally make use of various types of computers, router, switches and Laptops.

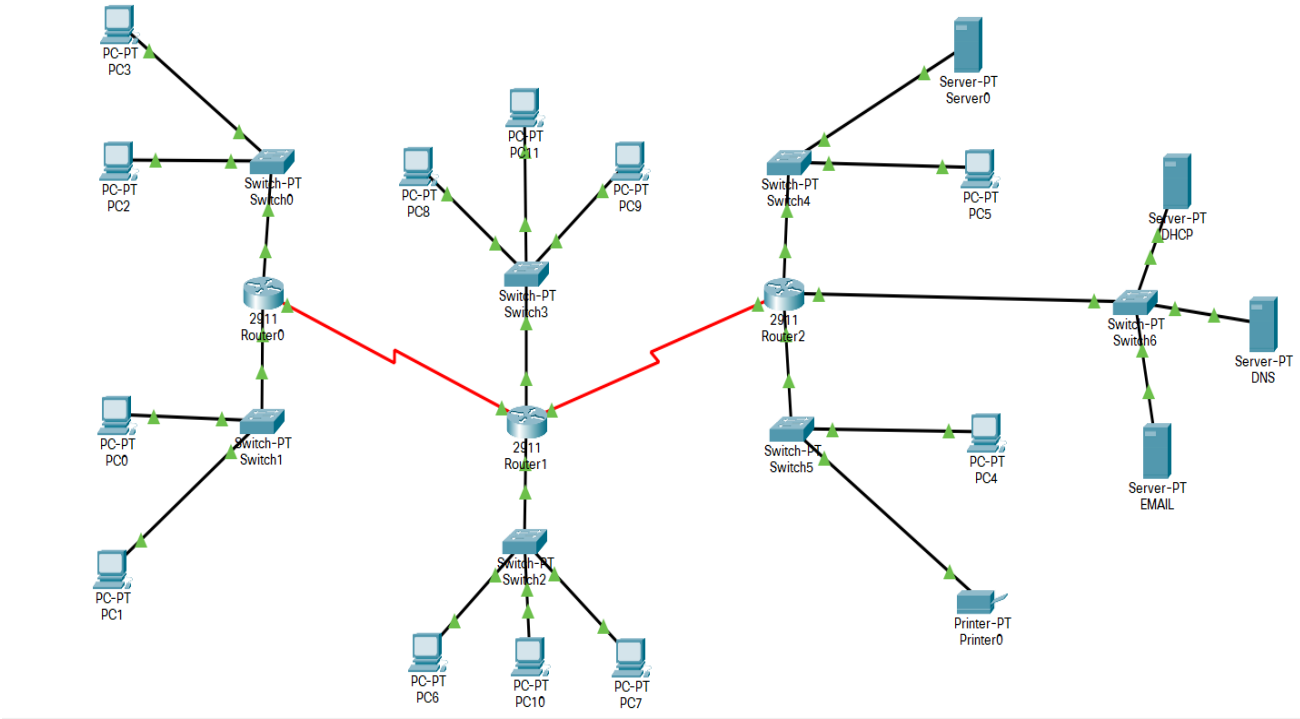

Fig. Architectural View of Network Design

Network Connectivity

In this Hospital Management System network the routers are connected with switch and switches are connected with laptops/computers.

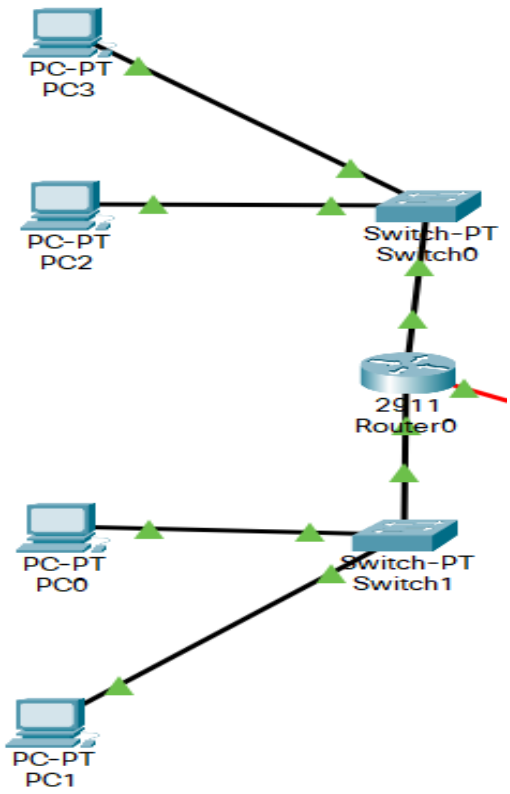

Fig. Connectivity of the Network

Ping Test

```
Packet Tracer PC Command Line 1.0
C:\>ping 199.168.10.2

Pinging 199.168.10.2 with 32 bytes of data:

Reply from 199.168.10.2: bytes=32 time=11ms TTL=128
Reply from 199.168.10.2: bytes=32 time=3ms TTL=128
Reply from 199.168.10.2: bytes=32 time=4ms TTL=128
Reply from 199.168.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 199.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 4ms

C:\>ping 199.168.10.255

Pinging 199.168.10.255 with 32 bytes of data:

Request timed out.
Reply from 199.168.10.1: bytes=32 time<1ms TTL=255
Reply from 199.168.10.1: bytes=32 time=13ms TTL=255
Reply from 199.168.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 199.168.10.255:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 4ms

C:\>
```

```
Packet Tracer PC Command Line 1.0
C:\>ping 196.168.10.4

Pinging 196.168.10.4 with 32 bytes of data:

Reply from 196.168.10.4: bytes=32 time=7ms TTL=128
Reply from 196.168.10.4: bytes=32 time=4ms TTL=128
Reply from 196.168.10.4: bytes=32 time=4ms TTL=128
Reply from 196.168.10.4: bytes=32 time=10ms TTL=128

Ping statistics for 196.168.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 10ms, Average = 6ms

C:\>ping 196.168.10.250

Pinging 196.168.10.250 with 32 bytes of data:

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

Ping statistics for 196.168.10.250:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

12. Summary

This report describes how we have designed network topology of hospital (Health care Management System) with VLSM for Subnetting. This topology can also be implemented on higher level of hospitals.

13. Reference

www.youtube.com - Jubaer Learning Tech

https://mocdoc.in/blog/a-detailed-view-of-hospital-management-system-hms - MocDoc

www.github.com - Suraj Kothari