

## **ABSTRACT**

### **1. Description of the problem and why it is being investigated:**

The project is carried out to establish an efficient way in which different wards can work fluently. Hospital can have access to high speed internet, hospital administrative can manage the different wards

### **2. The primary methods we use here are :**

TOOLS USED : CISCO PACKET TRACER

The technical services that have been placed in the hospital's network are failover firewalls utility, a Dynamic Host Configuration Protocol (DHCP) server, a Domain Name System (DNS) server and a cabling system. These tools can increase the performance of the network in general and provide a stable internet service. Also for patients's personal information safety, the web server has been placed in the local network, which provides a secure environment for any network's element.

### **3. Major results obtained from this project are:**

The project has been provided with different utilities to introduce a network with an integrated level of service for the hospital. These utilities are an IP access control list, a domain server and a proxy server, services by each provider, wifi service for the wards. All of these utilities have been configured to provide a secure environment for the entire network.

### **4. Conclusion of our results:**

The proposed system will provide enhanced security, scalability and high availability and will maintain the network in a better way.

## **INTRODUCTION**

A network proposal has to be designed for a hospital which has the following. There is a main block and three wards in the campus. The main block is the administrative block where registration of new patients takes place. The main block has 5 floors. The hospital has identified hospital management software, which should be accessible by the employees. The software is installed on a server at the administrative block. At the ground floor, there are 15 computers at the billing section. At other floors, there is one computer user each. The farthest distance between the computer on the top most floor and the ground floor is less than 70 meters. The wards have 5 floors each, with 10 computers in the ground floor of each ward. The distance between the wards and the blocks are less than 80

### **TOOLS USED**

- **Cisco Packet Tracer**

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.

- **StarUML**

StarUML is a UML tool by MKLab. The software was licensed under a modified version of GNU GPL until 2014, when a rewritten version 2.0.0 was released for beta testing under a proprietary license. After being abandoned for some time, the project had a revival to move from Delphi to Java/Eclipse and then stopped again

### **NETWORK REQUIREMENTS**

- Hardware requirement analysis in the main block with quantity.
- Hardware requirements analysis in wards.
- The employees should receive dynamic IP addressing from a central server.
- Network should be loop free at Layer 2
- Every computer should be able to access the hospital management software from each of the locations using a fixed IP address.
- IP Network design table.
- Identify configurations on the hardware wherever appropriate.

## **NETWORK REQUIREMENT ANALYSIS**

- In comparison SolarWinds Orion is more intuitive, easy to use and the best value network management solution.
- Matches and surpasses NetQos report analyzer capability.
- Complete visibility and control across network sites (various hospitals on the MAN), physical and virtual systems (Virtualization management and reporting), applications as well as Windows Event and Syslog monitoring to make not only rapid decisions and troubleshooting.
- Fault, configuration, traffic analysis, performance, security and compliance management as part of a complete solution.
- Proven in hundreds of thousands of medium to large enterprise business matrix, and service provider networks worldwide.
- 5 times less in cost than NetQos (Source Insight).
- Clear cut and user friendly to use compared to complex competitor solutions such as Ciscoworks and NetQos.
- Increased network availability and network device health more greens on the network.

## **HARDWARE REQUIREMENTS ANALYSIS**

- One router for each network transition. Internet – LAN or LAN – sub-network
- Most routers have 4 or 8 ports (connections) for sub-networks
- Most routers can process 100Mbps
- Servers that have high traffic (10Mbps-100Mbps) put on their own sub network
- Servers that have lower traffic (up to 10Mbps) put on their own port of a switch at a high level of the network hierarchy
- LAN with 8 or less computers creating low traffic could be connected to a hub
- LAN with 8 or less computers with one or more creating high traffic should be connected to a switch
- LAN with 9 or more computers should be connected by a switch
- Every networked computer requires a network card (adapter)
- Every wirelessly networked computer requires a wireless network adapter (some have built-in WiFi)
- One or more ports of a switch might be connected to other switches or hubs

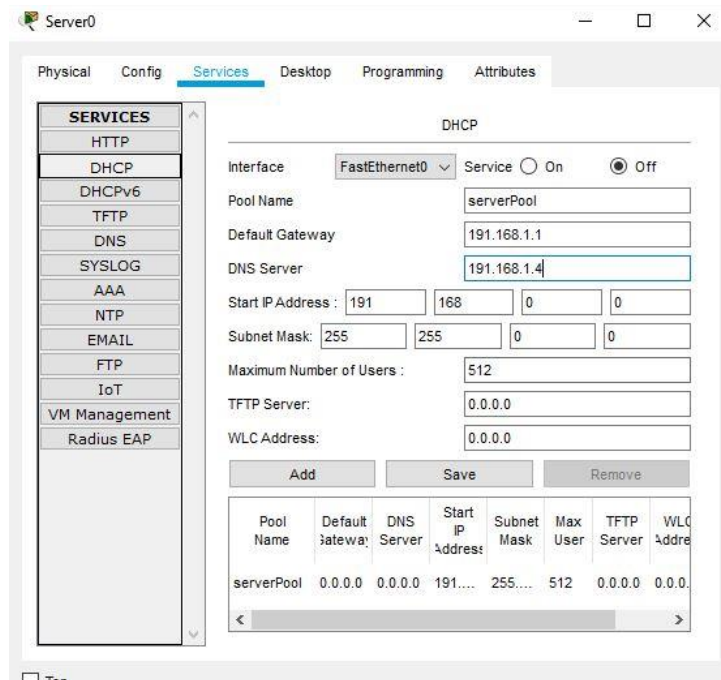
## **CONFIGURATIONAL GUIDELINES**

Guidelines for access-points and server configuration are discussed below:

- Access-points should be configured with security parameters to avoid the security risk.
- Dedicated services should be configured on servers to avoid any conflict between the departmental accesses to the network.
- VLANs should be properly added to the server to allow the communication between the devices.
- Security mechanisms should be implemented to secure the server-points from different types of attack

## Configure DHCP, DNS, HTTP Servers

**Step 1:** – Now, first of all, we configure DHCP Server so we can assign the automatic IP address on all other systems. To do so go to the DHCP server and open it. Now in the desktop menu go to IP configuration and assign IP statically to the server and also gives the DNS Server address as 1.0.0.2. The figure is shown below



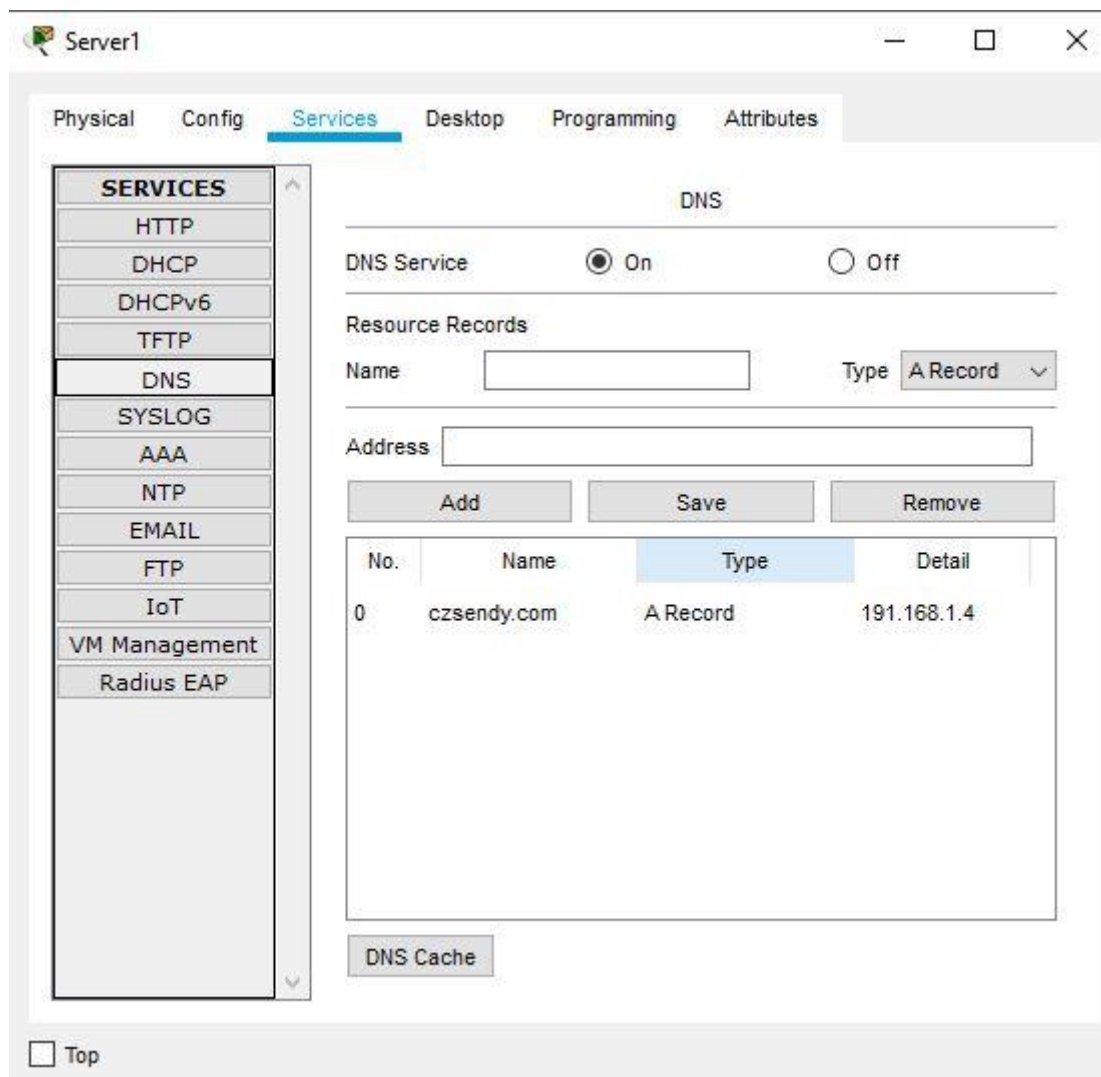
Server0 Configuration

**Step 2:** – Now to make this Server as DHCP Server we need to enable DHCP service on this Server. To do so go to its services menu and select DHCP in which fill the entries as your requirement and turn on the DHCP server by choosing the **ON** option from it. The figure is shown below

Now the work on the DHCP server is completed and DHCP Service is configured successfully. Now this Server is able to provide an IP address to the systems which are connected to this network

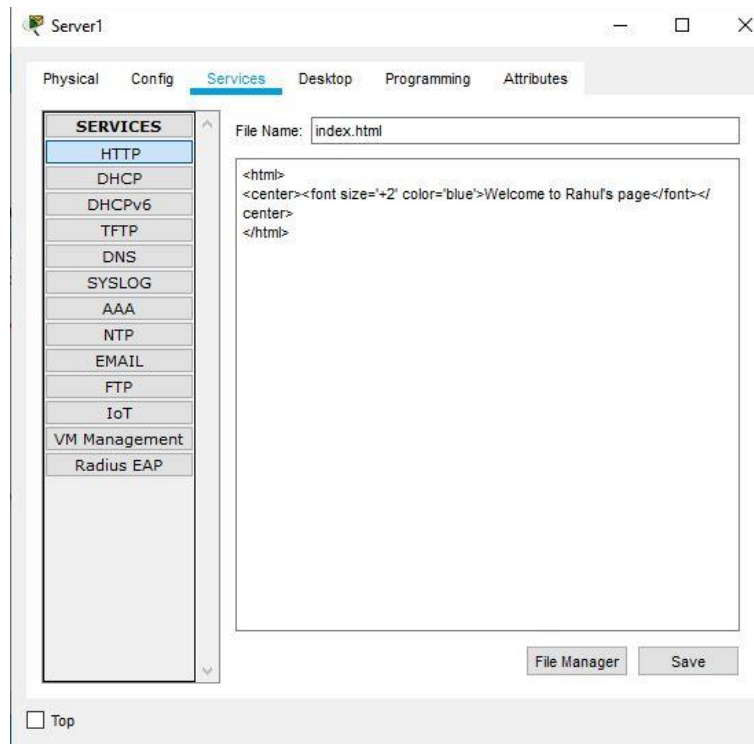
**Step 3:** – Now in next step we configure DNS Server so we can provide a medium in between HTTP Server and clients. To do so, first of all, select the DNS server after that in the desktop menu click on the IP configuration option and then change the IP Configuration method from Static to DHCP. Now you can observe that it will request for

an IP address from DHCP Server and an IP address is given automatically to the DNS server. The figure is shown below



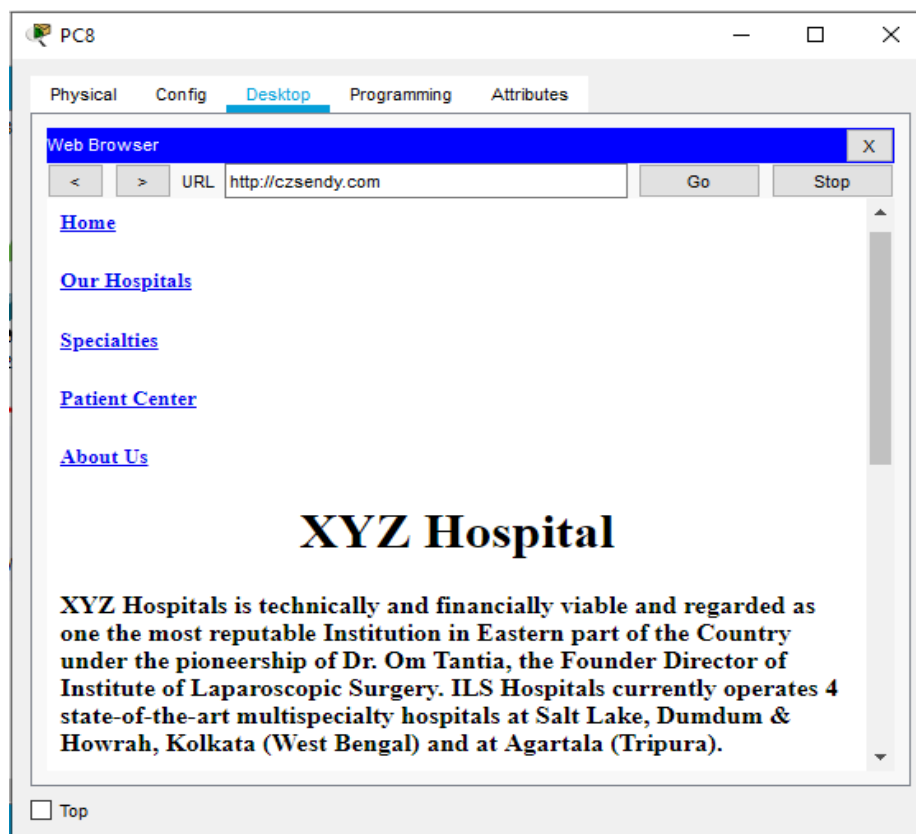
### Server1 DNS Configuration

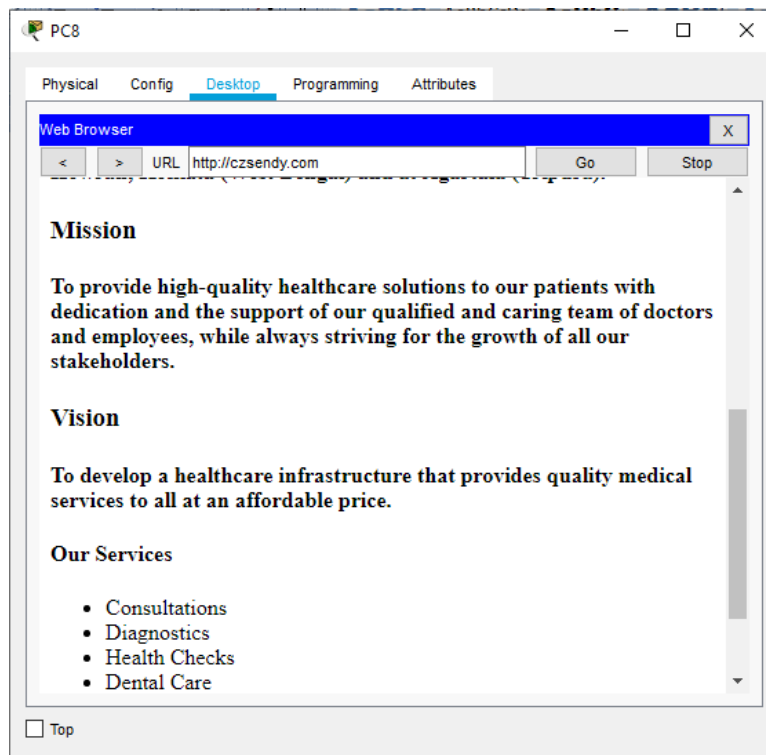
**Step 4:** – Now we configure DNS Services on this Server so we can provide a platform to make communication between Servers and clients. To do so go to services and select DNS then give the name and IP address of the HTTP Server as given below and click on the add button to add these entries in DNS Server. After that turn **ON** DNS Services on this Server.



### Server1 HTTP Configuration

**Step 5:** – Now to configure HTTP server on the next machine similarly as DNS server and DHCP Server. First of all, assign an IP address to it by using the DHCP server as given in step 4 and then go to HTTP in the services menu and create a page or edit a page that will be shown on the browser.

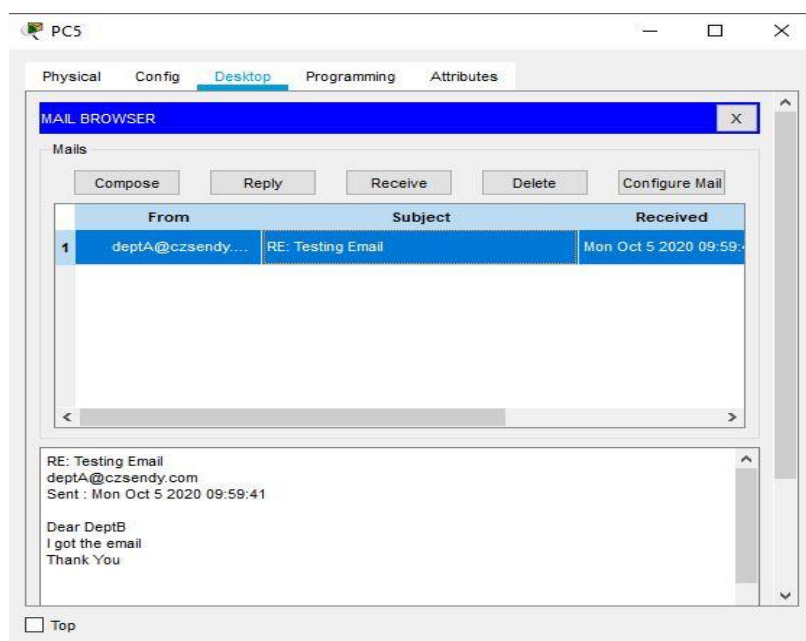




PC8 Webpage view

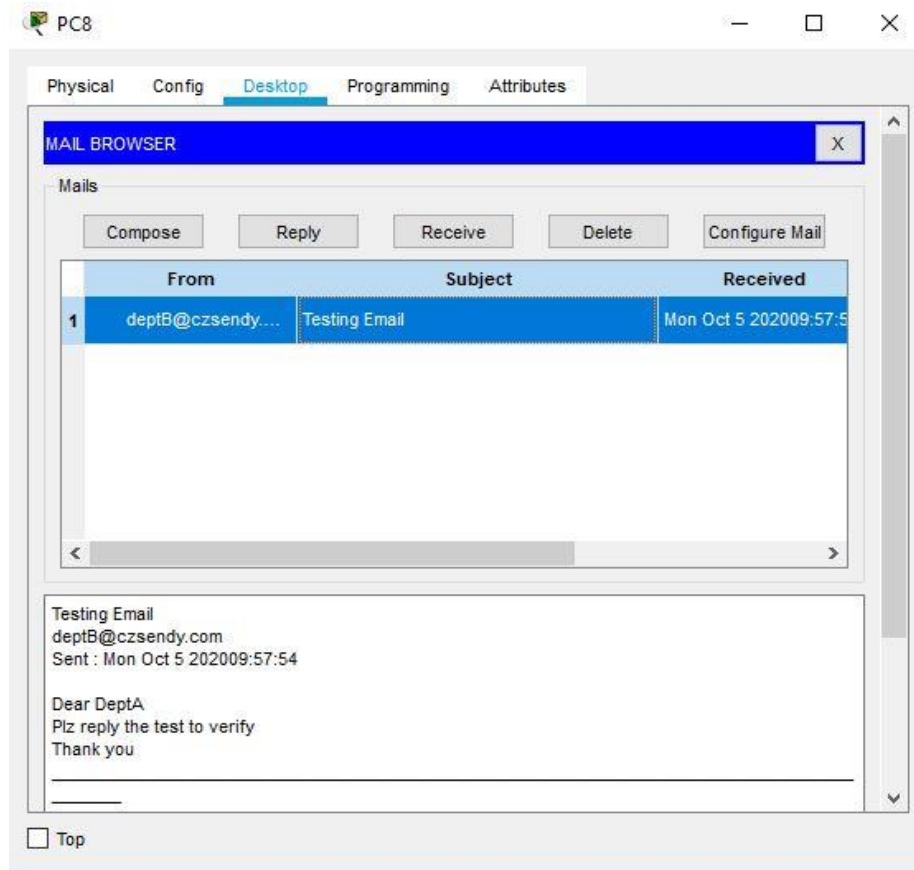
**Step 6:** – Now all the servers are configured. So, now we assign the IP address to the PCs using DHCP Server as given above. This is done because the client's request, first of all, goes to the DNS server where it directs it to the HTTP server and then webpage loads from HTTP server to our computer using the name instead of IP address.

**Step 7 :** Email Generation



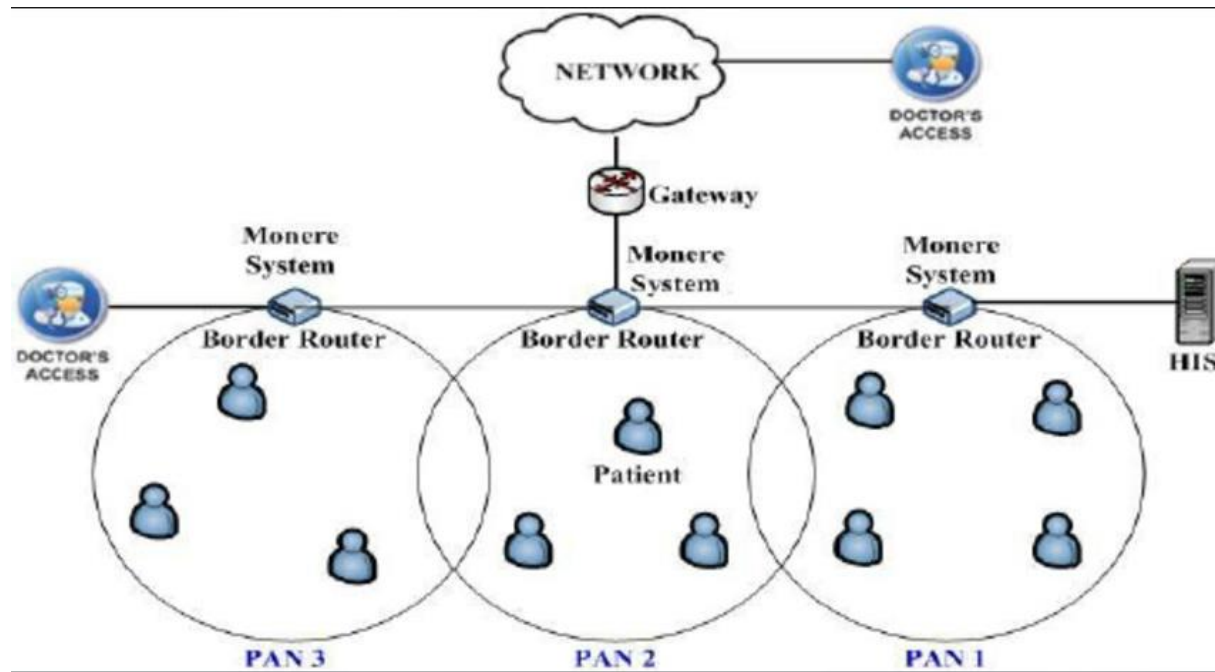
PC5 Email Generation





PC8 Email Receive and Reply

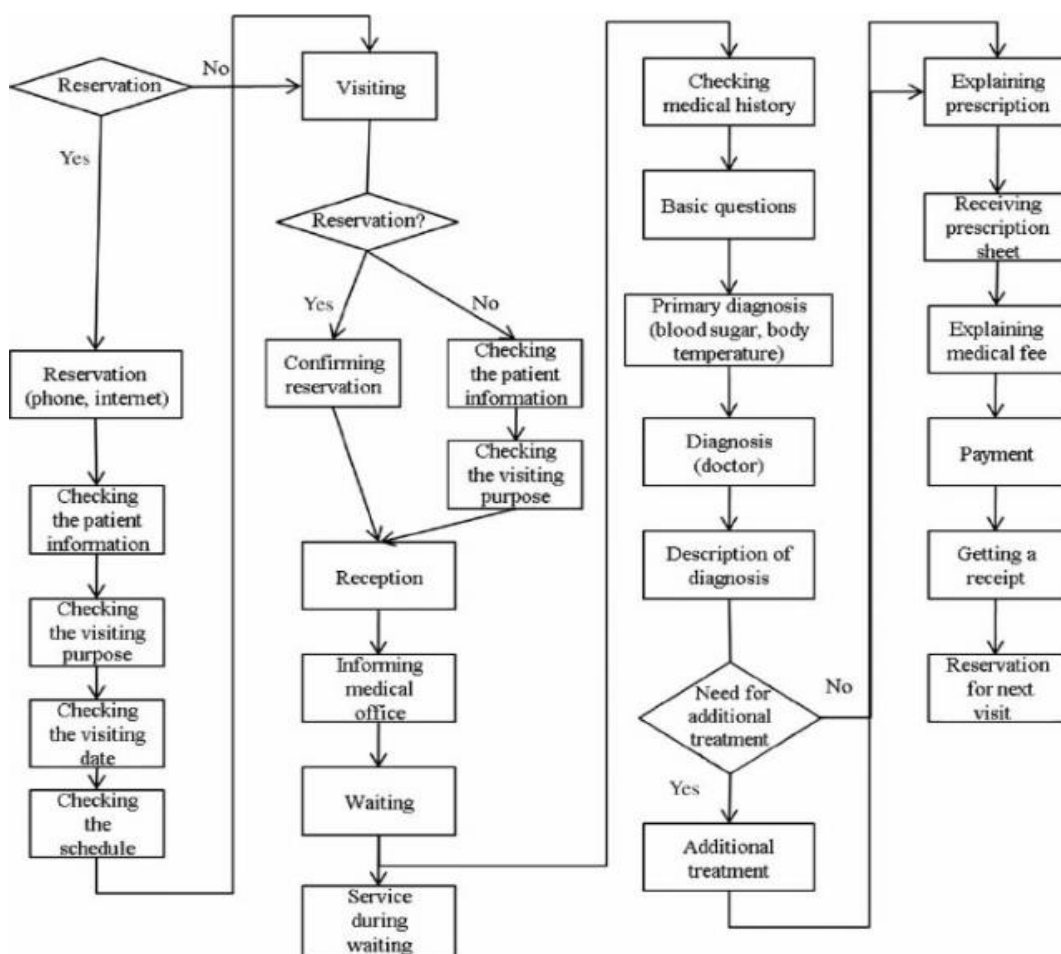
## Network topology diagram



Network Flow Diagram

## Cisco Packet Representation

### FLOW DIAGRAM



### Hospital Activity Flow Diagram

## **NETWORK TESTING AND VERIFICATION:**

As threats to cybersecurity increase and appear from unexpected new angles, a novel methodology is required to secure safe operations at sea. The possible impact of failures and vulnerabilities calls for action.

The integrated approach for handling software and software updates is essential for safe operations. Inherent to most industrial control systems today is the design perspective that programmable logic controllers (PLCs), and the network infrastructure interconnecting them, operate in a secure environment sealed from malicious attackers.

The first step towards securing control systems is to make sure PLCs are designed and operated according to recognized international standards and recommendations such as the ISO 27000 series, the NOG 104 guidelines and the NIST 800, among others.

DNV GL helps to secure the safety and integrity of industrial control systems by probing these networks for possible vulnerabilities and testing their robustness, to verify that the implementation of the design is safe, secure and carried out in accordance with the documentation.

The overall scope of cybersecurity and network resilience testing from DNV GL covers:

- Stress and robustness testing
- Penetration testing and testing of network segregation
- Screening running services, patches and firmware
- Authentication weaknesses
- Portable media security
- Known and unknown vulnerabilities
- Traffic anomalies
- Degradation of networked equipment
- Protect your network with the help of DNV GL cybersecurity services:
- Know where vulnerabilities are to safeguard your system against a malicious hacker, disgruntled employee or hardware/software failure

- Benefit from our insights into critical parts of control system networks and IT architecture to secure the integrity of control systems and hereby the safety and security of your operation.

## **CONCLUSION**

Thus a Hospital Network Server is established by maintaining Security and Privacy of the organisation as mentioned in the above result. All of these utilities have been configured to provide a secure environment for the entire network. The proposed system will provide enhanced security, scalability and high availability and will maintain the network in a better way. The hospital has identified hospital management software, which should be accessible by the employees. The software is installed on a server at the administrative block. At the ground floor, there are 15 computers at the billing section. At other floors, there is one computer user each. The farthest distance between the computer on the top most floor and the ground floor is less than 70 meters. The wards have 5 floors each, with 10 computers in the ground floor of each ward. The distance between the wards and the blocks are less than 80

## **INFERENCES:**

The project is carried out to establish an efficient way in which different wards can work fluently. Hospital can have access to high speed internet, hospital administrative can manage the different wards. The technical services that have been placed in the hospital's network are failover firewalls utility, a Dynamic Host Configuration Protocol (DHCP) server, a Domain Name System (DNS) server and a cabling system. These tools can increase the performance of the network in general and provide a stable internet service. Also for patients's personal information safety, the web server has been placed in the local network, which provides a secure environment for any network's element.

The project has been provided with different utilities to introduce a network with an integrated level of service for the hospital. These utilities are an IP access control list, a domain server and a proxy server, services by each provider, wifi service for the wards. All of these utilities have been configured to provide a secure environment for the entire network. The proposed system will provide enhanced security, scalability and high availability and will maintain the network in a better way.