**MINOR PROJECT REPORT**

***on***

# Secured Server Room Design

**For**

**18ECP107L / Minor Project**

***Submitted by***

Y. Prameya (RA1911004010580)

K.N.Varma (RA1911004010587)

D. Sudheer (RA1911004010598)

**Semester – VII**
**Academic Year: 2022-23**

***Under the supervision of***

**Mr. S. Manikandaswamy:** Asst Professor, Department of ECE

**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING**

**College of Engineering and Technology,**

**SRM Institute of Science and Technology**

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamil Nadu.

**NOV 2022**

# SRM Institute of Science and Technology

(Under Section 3 of UGC Act, 1956)

## BONAFIDE CERTIFICATE

Certified that this project report titled "**SECURED SERVER ROOM DESIGN**" is the bonafide work of "Y. PRAMEYA [Reg No: RA1911004010580], K. N. VARMA [Reg No: RA1911004010587], D. SUDHEER [ Reg No: RA1911004010598],", who carried out the project work under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

***SIGNATURE***

**Mr. S. Manikandaswamy**
Assistant Professor,
Dept. of Electronics &
Communication Engineering

***SIGNATURE***

**Dr. M S Vasanthi**
Associate Professor,
Dept. of Electronics &
Communication Engineering

# ABSTRACT

Computer networks have become increasingly ubiquitous and there is a demand for securing the data over the networks. All the servers are organized in such a way that it is responsible for file transfer, remote login via ssh, time, emails, http web pages, DNS and configured DHCP for the lab. In this project, the security of the server system is secured strongly by implementing the syslog server. The unauthorized users are denied by this server by strong encrypting algorithms used for login to the servers and the network id’s are masked. Network gets extra security so that no one can configure the network or servers for any purpose without the perfect combination from the administrator. By implementing the syslog server, we can achieve the better security on the network.

# ACKNOWLEDGEMENTS

We would like to express our deepest gratitude to our guide, name Mr. S. Manikandaswamy, Assistant Professor, Department of Electronics and Communication Engineering for his valuable guidance, consistent encouragement, personal caring, timely help and providing us with an excellent atmosphere for doing project. All through the work, in spite of his busy schedule, he has extended cheerful and cordial support to us for completing this project work.

# TABLE OF CONTENTS

| S.NO | Contents | Page no |
|---|---|---|
| 1 | ABSTRACT | 3 |
| 2 | ACKNOWLEDGEMENTS | 4 |
| 3 | ABBREVIATIONS | 7 |
| 4 | INTRODUCTION<br>1. PROBLEM STATEMENT<br>2. OBJECTIVE<br>3. REQUIREMENTS | 8 |
| 5 | LITERATURE SURVEY | 9 |
| 6 | PROPOSED SYSTEM | 10 |
| 7 | DESIGN METHODOLOGY | 11-15 |
| 8 | CONCLUSION | 16 |
| 9 | FUTURE WORK | 17 |
| 10 | APPENDIX | 18-20 |
| 11 | REFERENCES | 21 |

# TABLE OF FIGURES

| FIGURE NO | NAME | PAGE NO |
|---|---|---|
| 1.1 | Server room design | 10 |
| 1.2 | Email service | 11 |
| 1.3 | HTTP service | 12 |
| 1.4 | FTP service | 12 |
| 1.5 | DNS service | 13 |
| 1.6 | Syslog service | 13 |
| 1.7 | NTP service | 14 |
| 1.8 | DHCP service | 15 |
| 1.9 | Administrative distances | 20 |

# ABBREVIATIONS

- SMTP - Simple Mail Transfer Protocol
- HTTP/HTTPS - Hypertext Transfer Protocol
- FTP - File Transfer Protocol
- TFTP - Trivial File Transfer Protocol
- DNS - Domain Name System
- SYSLOG - System Logging Protocol
- NTP - Network Time Protocol
- DHCP - Dynamic Host Configuration Protocol
- IP - Internet Protocol
- SSH - Secure Shell
- TELNET - Teletype Network Protocol

# INTRODUCTION

## PROBLEM STATEMENT

- Attacks and security on server room has been a threatening issue. Several methods have been introduced to defend the situations. Hence, we are up with secure server room design model.

## OBJECTIVE

- To design secure server room using cisco packet tracer.
- To implement syslog server for analyzing network traffic.
- To introduce security on routers using MD5 encryption algorithm.

## REQUIREMENTS

- **SOFTWARE** Cisco Packet Tracer

  Server, Routers, P.C's, Laptop, Wires, Switches

# LITERATURE SURVEY

[1] Title: Server Designs for Warehouse
Authors: K. Lim, P. Ranganathan
Published in: IEEE Micro (Volume: 29, Issue: 1, Jan.-Feb. 2009)
Inference: The enormous scale of warehouse computing environments leads to unique requirements in which cost and power figure prominently. Models and metrics quantifying these requirements, along with a benchmark suite to capture workload behavior, help identify bottlenecks and evaluate solutions.

[2] Title: Data safety audit in small and medium-sized enterprises
Authors: Marek Sikora, Grzegorz dzieża, marcin jasiński
Published in: ResearchGate 2017
Inference: The policy of data protection is belittled in many companies. Appropriate data storage is not sufficient enough –there is also a need for the right policy of protecting data which will ensure a fast access to the crucial information in case of a critical failure.

[3] Title: Secure Server
Authors: Markus Jakobsson, Susanne Wetzel
Published in: International Workshop on Public Key Cryptography PKC 2001: Public Key Cryptography pp 383–401
Inference: We study how to reduce the local computational cost associated with performing exponentiation. This involves transforming a large computational task into a large set of small computational tasks that are to be performed by a set of external servers who may all be controlled by one and the same adversary. In order to attack our problem, we introduce and employ the three principles of duplication, distribution and delegation.

[4] Title: Database Security
Authors: Rodney Compton
Published in: International Conference on smfmarine 2011
Inference: The goal is to keep a database server secure. Protection for these database servers start at the physical level. Having a secured server room where only authorized individuals may access the room is key

# PROPOSED SYSTEM

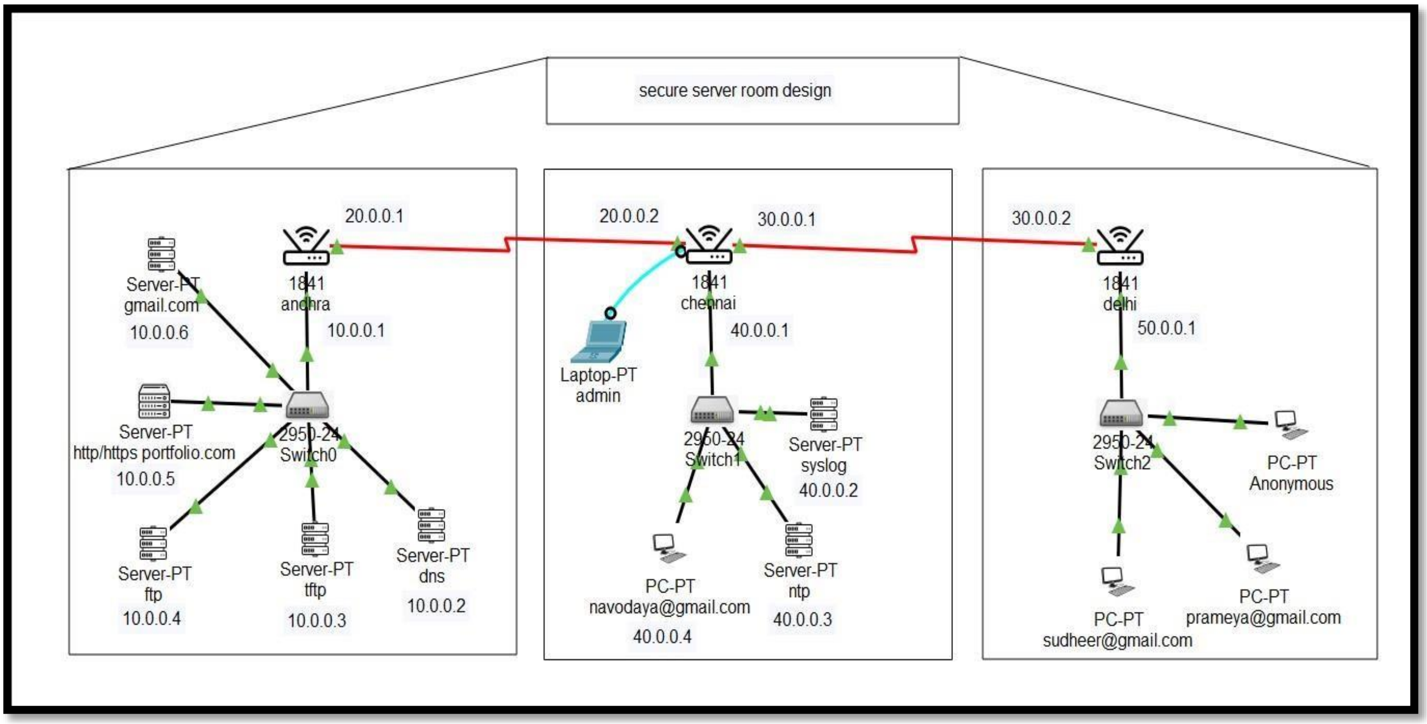


Fig 1.1 Server room design

Configured Server room in two locations and build a testing Lab in another location. Design was created as follows.

- **Location 1 (Andhra)**
  - ✓ Configured ftp server and tftp server.
  - ✓ Transferred config files to remote server(ftp) for back up.
  - ✓ Implemented ntp server on network for time sync.
  - ✓ Configured Telnet Usernames and passwords for remote login via ssh.
- **Location 2 (Chennai)**
  - ✓ Configured Syslog server on this router as it is an centralized router in the network.
  - ✓ Introduced Security for Console and Aux ports of router.
  - ✓ Configured Telnet Usernames and passwords for remote login via ssh.
  - ✓ Implemented MD5 encryption algorithm.
  - ✓ Added Description and Banner for the router.
- **Lab (Delhi)**
  - ✓ Configured DHCP on the Network, which is responsible for getting network parameters dynamically.
  - ✓ Transferred config files to remote server(tftp) for back up.

# DESIGN METHODOLOGY

Implemented static routing while configuring the server room in two locations because-

- ✓ Static routing causes very little load on the CPU of the router, and produces no traffic to other routers.
- ✓ Static routing leaves the network administrator with full control over the routing behaviour of the network.
- ✓ Static Routing Is very easy to configure on small networks.
- ✓ When two or more routing protocols was enabled, it will follow Static routing since its administrative distance is 0

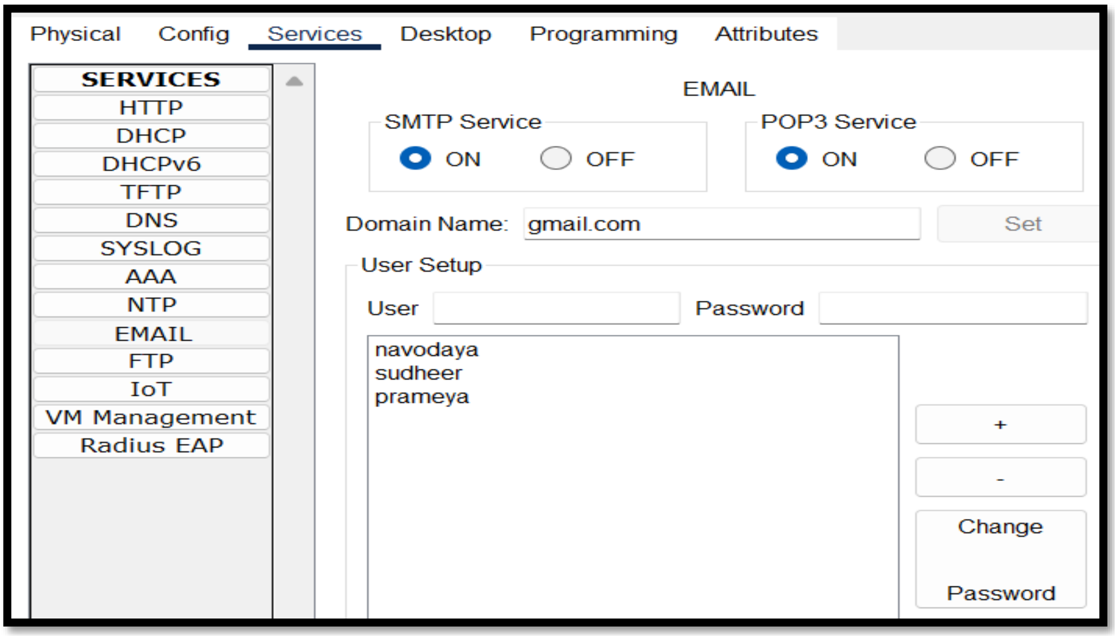
## Location1(andhra)

Services configured in Location1 are-

- ✓ SMTP
- ✓ HTTP/HTTPS
- ✓ FTP
- ✓ TFTP
- ✓ DNS

### SMTP

Initially we have to enable the smtp service on server and have to create usernames and passwords for communication over networks and it also depends on DNS.



EMAIL

SMTP Service: ● ON ○ OFF

POP3 Service: ● ON ○ OFF

Domain Name: gmail.com

User Setup

User

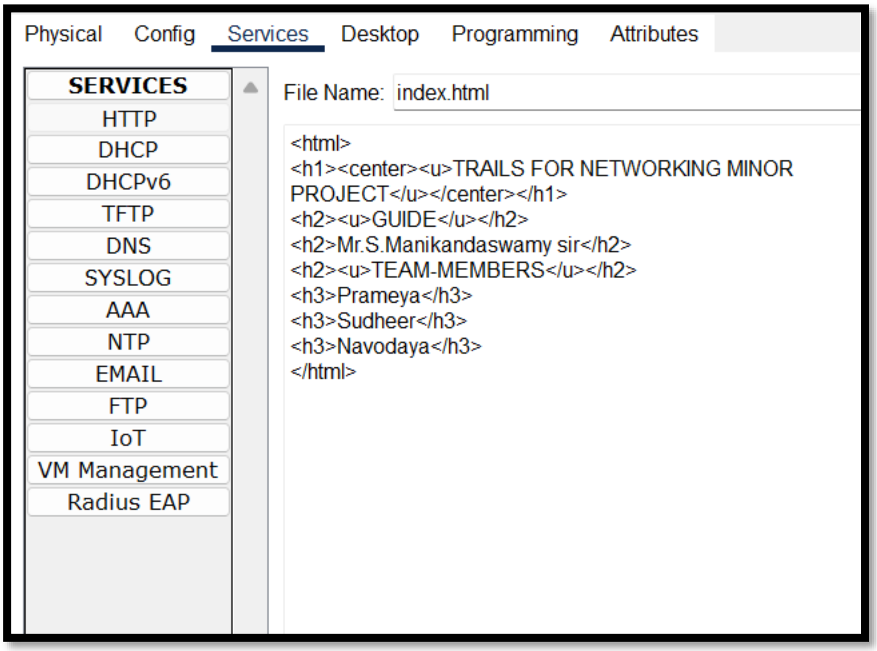
Password

navodaya
sudheer
prameya

Fig 1.2 Email Service

## HTTP/HTTPS

For this service we initially created an index.html file and named in DNS as portfolio.com for accessing over the networks.



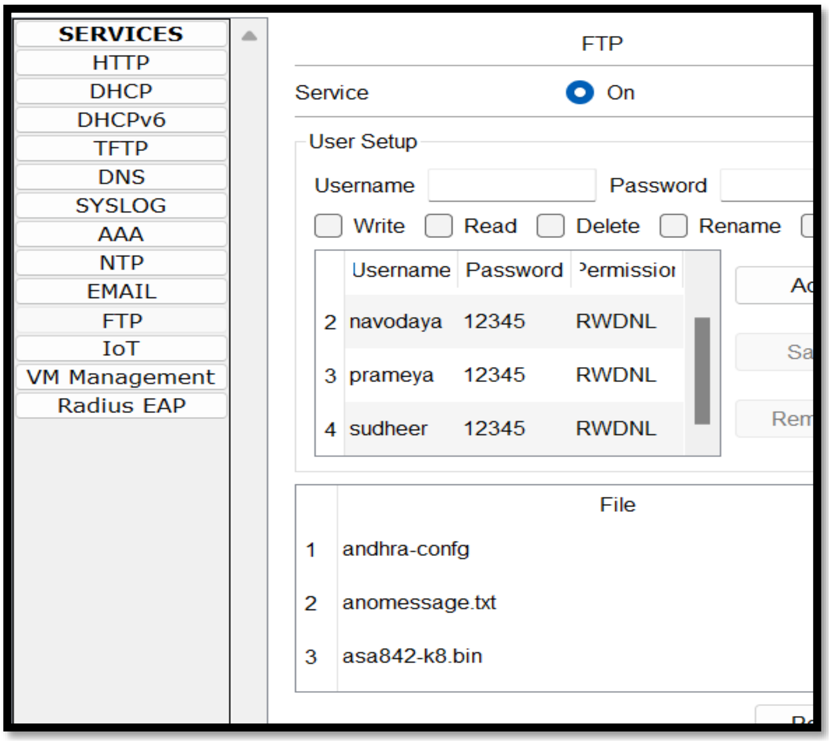
File Name: index.html

```
<html>
<h1><center><u>TRAILS FOR NETWORKING MINOR
PROJECT</u></center></h1>
<h2><u>GUIDE</u></h2>
<h2>Mr.S.Manikandaswamy sir</h2>
<h2><u>TEAM-MEMBERS</u></h2>
<h3>Prameya</h3>
<h3>Sudheer</h3>
<h3>Navodaya</h3>
</html>
```

Fig 1.3 HTTP Service

## FTP

For enabling the ftp service in the network, we have to enable the ftp service on the server and have to create usernames and passwords and have to manually enter the ftp commands on each router.



Service ● On

|  | Username | Permissio |
|---|---|---|
| 2 | navodaya | 12345 | RWDNL |

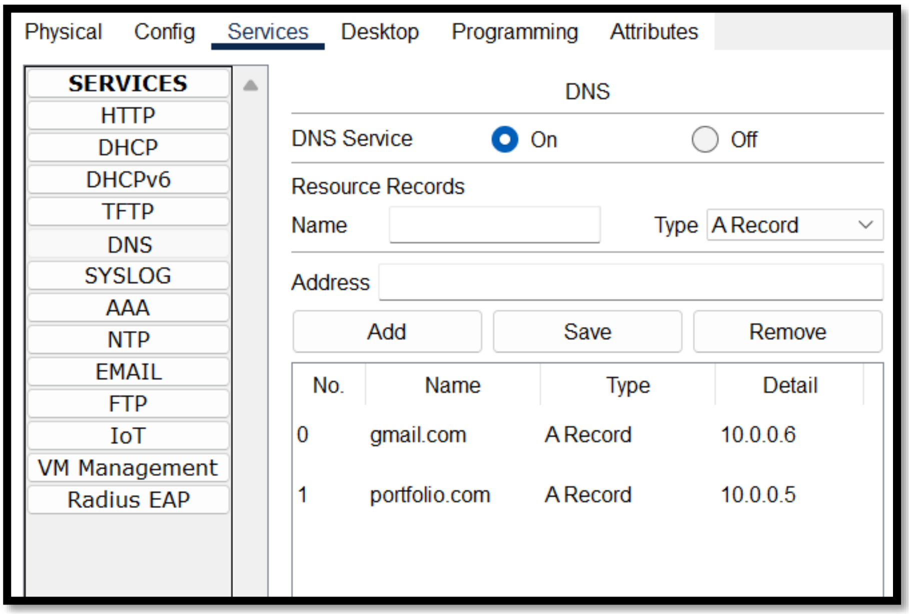
| | Username | Password | Permissio |
|---|---|---|---|
| 2 | navodaya | 12345 | RWDNL |
| 3 | prameya | 12345 | RWDNL |
| 4 | sudheer | 12345 | RWDNL |

| | File |
|---|---|
| 1 | andhra-confg |
| 2 | anomessage.txt |
| 3 | asa842-k8.bin |

Fig 1.4 FTP Service

## DNS

With this server we can assign a name to a particular domain and can be accessed over the network without the need of an ip address.



DNS

DNS Service ● On ○ Off

Resource Records

Name Type A Record

Address

| No. | Name | Type | Detail |
|---|---|---|---|
| 0 | gmail.com | A Record | 10.0.0.6 |
| 1 | portfolio.com | A Record | 10.0.0.5 |

Fig 1.5 DNS Service

## Location2 (Chennai)

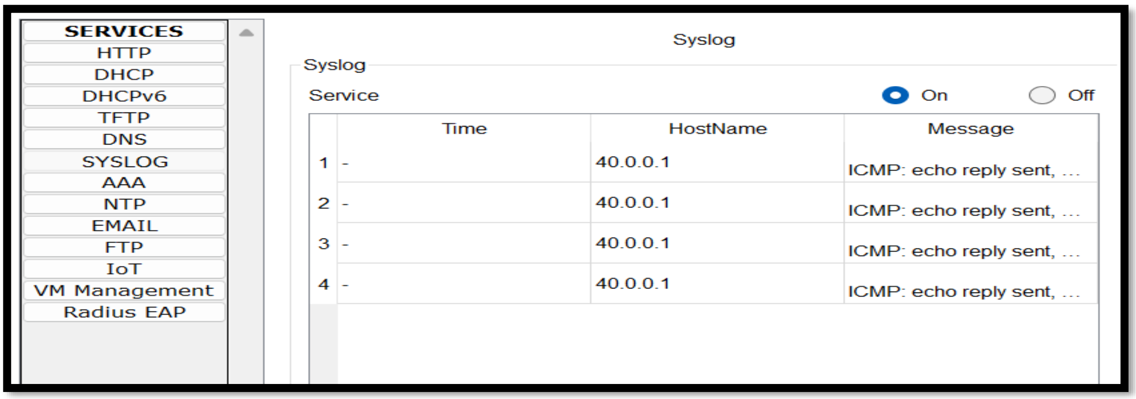
Services configured in Location2 are-

- ✓ Syslog
- ✓ NTP

## Syslog

With this server we can monitor the network traffic and this can be enabled by going to services on the server and can be taped by giving the following CLI commands.

```
chennai(config)#logging host 40.0.0.2
chennai(config)#logging trap debugging
chennai(config)#exit
chennai#debug ip  icmp
ICMP packet debugging is on
```



Syslog

Syslog

Service ● On ○ Off

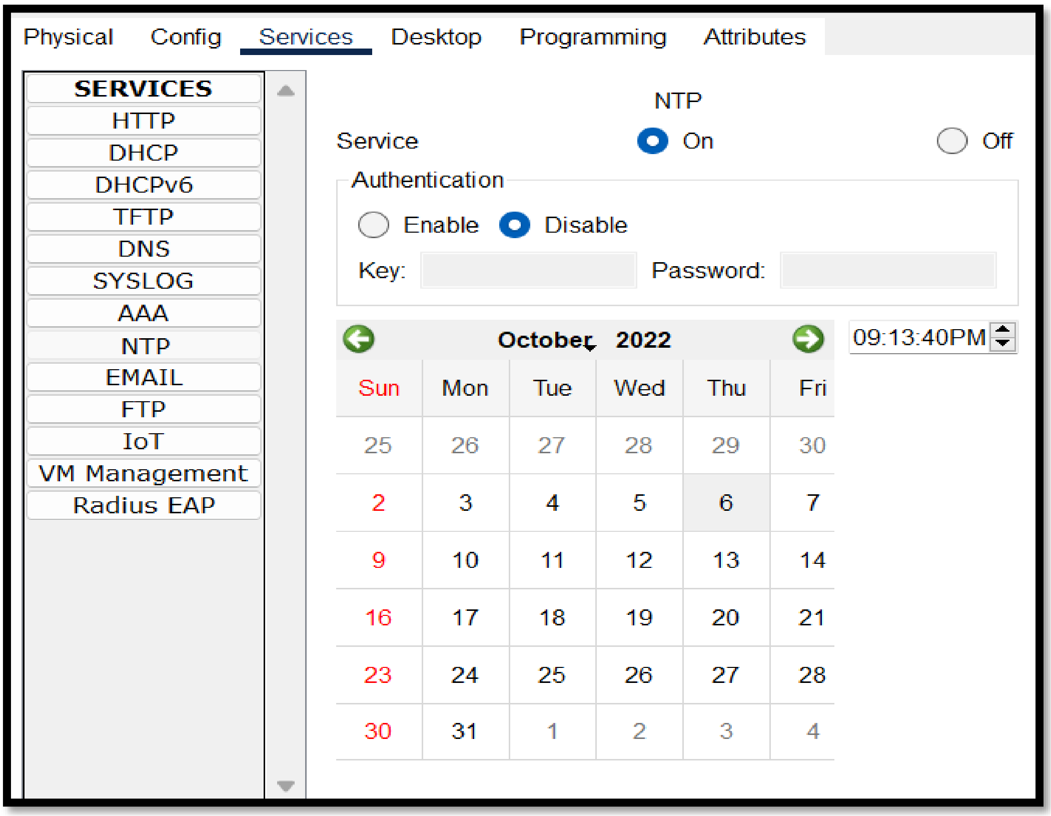
| | Time | HostName | Message |
|---|---|---|---|
| 1 | - | 40.0.0.1 | ICMP: echo reply sent, ... |
| 2 | - | 40.0.0.1 | ICMP: echo reply sent, ... |
| 3 | - | 40.0.0.1 | ICMP: echo reply sent, ... |
| 4 | - | 40.0.0.1 | ICMP: echo reply sent, ... |

Fig 1.6 Syslog service

## NTP

With this ntp server we can able to sync the time over the network this can be enabled by checking on the ntp service on the server. and by giving the following CLI commands on the routers.

```
andhra(config)#ntp server 40.0.0.3
andhra(config)#exit
```



NTP

Service ● On ○ Off

Authentication

○ Enable ● Disable

Key: Password:

October 2022 09:13:40PM

| Sun | Mon | Tue | Wed | Thu | Fri |
|---|---|---|---|---|---|
| 25 | 26 | 27 | 28 | 29 | 30 |
| 2 | 3 | 4 | 5 | 6 | 7 |
| 9 | 10 | 11 | 12 | 13 | 14 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 23 | 24 | 25 | 26 | 27 | 28 |
| 30 | 31 | 1 | 2 | 3 | 4 |

Fig 1.7 NTP Service

## Location3 (Delhi)

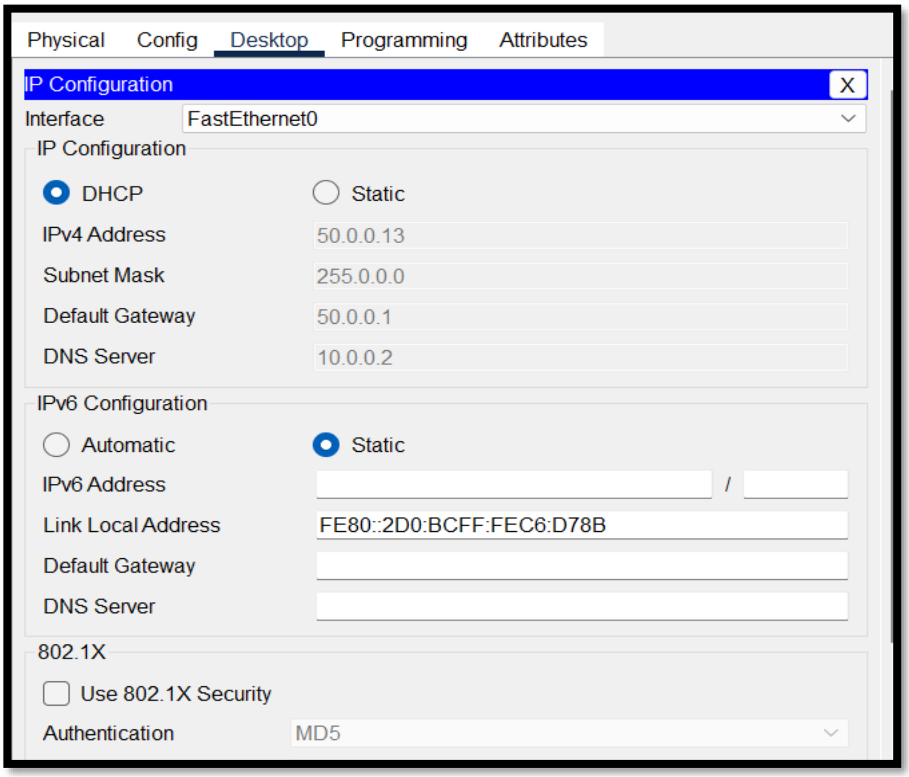
Services configured in Location3 are-

- ✓ DHCP

## DHCP

With this service we can dynamically allocate the ip address, DNS server and default gateways automatically on connection. By giving the following CLI commands on the router.

```
delhi(config)#ip dhcp excluded-address 50.0.0.1 50.0.0.12
delhi(config)#ip dhcp pool room1
delhi(dhcp-config)#default-router 50.0.0.1
delhi(dhcp-config)#dns-server 10.0.0.2
delhi(dhcp-config)#network 50.0.0.0 255.0.0.0
```



IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 50.0.0.13

Subnet Mask: 255.0.0.0

Default Gateway: 50.0.0.1

DNS Server: 10.0.0.2

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::2D0:BCFF:FEC6:D78B

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

Fig 1.8 DHCP Service

## TELNET

It allows a user to establish a remote connection to a system in a way that makes it appear as a local system via the command line. SSH is an open-source network protocol used to access and manage devices remotely via a program. By giving the following CLI commands on the router.

```
andhra(config)#username navodaya password 12345
andhra(config)#username sudheer password 12345
andhra(config)#username prameya password 12345
andhra(config)#
andhra(config)#line vty 0 5
andhra(config-line)#login local
andhra(config-line)#exit
```

# CONCLUSION

- The proposed design provides a tight security on the network and traffic is monitored by syslog server continuously.
- Authorized users can access the network depending on their permissions.
- It effectively monitors traffic on the network and it provides services such as EMAIL, FTP, HTTP/HTTPS, DNS, DHCP.

# FUTURE WORK

- Network can be monitor continuously by configuring IOT devices.
- Network administrator can be dynamically notified if there is congestion in network traffic.
- By implementing Machine Learning models unauthorized users in the server room can be identified.

# APPENDIX

## ➢ FTP SERVER AND TFTP SERVER

FTP is a widely used protocol that allows the remote user to navigate the server's file structure and upload and download files. TFTP is a simplified alternative to FTP that provides no authentication and is most often used to transfer configurations to and from network devices.

- ✓ FTP works on two ports: 20 and 21. While TFTP works on 69 Port number.

## ➢ NTP SERVER OR TIME SERVER

The Network Time Protocol (NTP) is used by hundreds of millions of computers and devices to synchronize their clocks over the Internet. If your computer sets its own clock, it likely uses NTP.

- ✓ NTP is a built-on UDP, where port 123 is used for NTP server communication and NTP clients use port 1023 (for example, a desktop).

## ➢ SYSLOG OR LOG SERVER

Syslog is a standard protocol for message logging that computer systems use to send event logs to a Syslog server for storage. On network devices, Syslog can be used to log events such as changes in interface status, system restarts, etc. A lot of different types of events can be logged.

- ✓ The default protocol for sending syslogs is UDP with a default port of 514. For TCP, the default port is 601. By default, the logging severity of syslogs is informational which means all syslogs at informational severity and higher will be logged.

## ➢ TELNET AND SSH

Telnet is a TCP/IP protocol that allows a user to establish a remote connection to a system in a way that makes it appear as a local system via the command line. SSH is an open-source network protocol used to access and manage devices remotely via a program.

- ✓ The default port for SSH client connections is 22; The default port for Telnet client connections is 23; to change this default, enter a port number between 1024 and 32,767.

- **HTTP/HTTPS**

The Hypertext Transfer Protocol is an application protocol for distributed, collaborative, hypermedia information systems that allows users to communicate data on the World Wide Web. HTTP was invented alongside HTML to create the first interactive, text-based web browser: the original World Wide Web. Today, the protocol remains one of the primary means of using the Internet.

- ✓ The default HTTP and HTTPS ports for the Web server are port 80 and 443, respectively.

- **SMTP**

SMTP is used to send and receive email. It is sometimes paired with IMAP or POP3 (for example, by a user-level application), which handles the retrieval of messages, while SMTP primarily sends messages to a server for forwarding.

- ✓ Port 25 is the original standard email SMTP port and the oldest, since it first debuted in 1982.

- **DNS SERVER**

Domain Name System (DNS) Server is a server that is specifically used for matching website hostnames (like example.com) to their corresponding Internet Protocol or IP addresses. The DNS server contains a database of public IP addresses and their corresponding domain names.

- ✓ DNS is mostly UDP Port 53, but as time progresses, DNS will rely on TCP Port 53 more heavily.

- **DHCP SERVER**

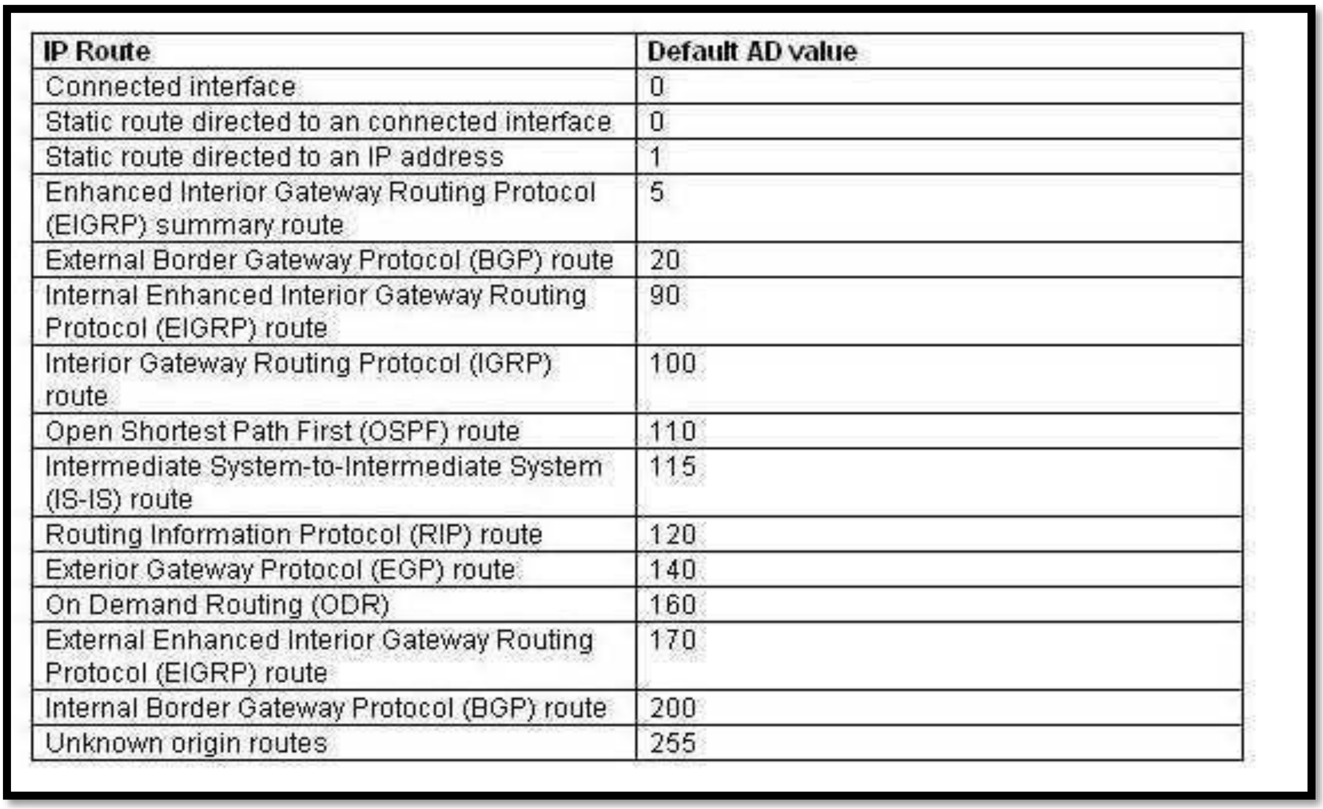
A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients.

- ✓ UDP port number 67 is the port used by the server, and UDP port number 68 is used by the client.

- **ADMINISTRATIVE DISTANCE**

Administrative distance is the first criterion that a router uses to determine which routing protocol to use if two protocols provide route information for the same destination. Administrative distance is a measure of the trustworthiness of the source of the routing information. Administrative distance has only local significance, and is not advertised in routing updates.

Note: The smaller the administrative distance value, the more reliable the protocol. For example, if a router receives a route to a certain network from both Open Shortest Path First (OSPF) (default administrative distance - 110) and Interior Gateway Routing Protocol (IGRP) (default administrative distance - 100), the router chooses IGRP because IGRP is more reliable. This means the router adds the IGRP version of the route to the routing table.



| IP Route | Default AD value |
|---|---|
| Connected interface | 0 |
| Static route directed to an connected interface | 0 |
| Static route directed to an IP address | 1 |
| Enhanced Interior Gateway Routing Protocol (EIGRP) summary route | 5 |
| External Border Gateway Protocol (BGP) route | 20 |
| Internal Enhanced Interior Gateway Routing Protocol (EIGRP) route | 90 |
| Interior Gateway Routing Protocol (IGRP) route | 100 |
| Open Shortest Path First (OSPF) route | 110 |
| Intermediate System-to-Intermediate System (IS-IS) route | 115 |
| Routing Information Protocol (RIP) route | 120 |
| Exterior Gateway Protocol (EGP) route | 140 |
| On Demand Routing (ODR) | 160 |
| External Enhanced Interior Gateway Routing Protocol (EIGRP) route | 170 |
| Internal Border Gateway Protocol (BGP) route | 200 |
| Unknown origin routes | 255 |

Fig 1.9 Administrative Distances

# REFERENCES

- Alaa H. Ahmed and Mokhaled N. A. Al-Hamadani "Designing a secure campus network and simulating it using Cisco packet tracer" Indonesian Journal of Electrical Engineering and Computer Science 23(1):479-489 (July 2021) https://www.researchgate.net/profile/Mokhaled-Al-Hamadani/publication/353380964_Designing_a_secure_campus_network_and_simulating_it_using_Cisco_packet_tracer/links/60f961991e95fe241a7d9d33/Designing-a-secure-campus-network-and-simulating-it-using-Cisco-packet-tracer.pdf

- K. Kranthi Kumar, E. Ramaraj, B. Srikanth, A. Srinivasa Rao, PBVN Prasad "Role of MD5 Message-Digest Algorithm for Providing Security to Low-Power Devices" published in IEEE on 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS) (June 2022) https://ieeexplore.ieee.org/abstract/document/9788249

- Aisha Muhammad, Aisha Abdulrahman Abba, Kashim Kyari Mohammed, Abuhuraira Abubakar "Enterprise Network Design and Implementation using Cisco Packet Tracer" (December 2020) https://hozir.org/pars_docs/refs/558/557724/557724.pdf