

A Mini Project Report on

Cyber Cafe Network

Submitted in partial fulfillment of the requirements
of the Semester VII Subject of

Network Design Lab

in

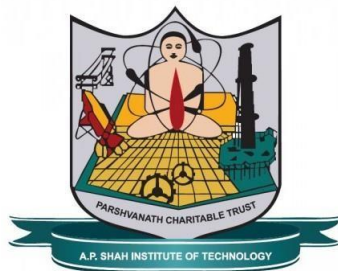
Information Technology

by

Krishita Tolia (18104021)
Siddhesh Gaikwad (18104069)
Akshata Gawas (18104039)

Subject Incharge

Prof.Sonal Jain



Department of Information Technology

A.P. Shah Institute of Technology
G.B.Road,Kasarvadavli, Thane(W), Mumbai-400615
UNIVERSITY OF MUMBAI
2021-2022

CERTIFICATE

This is to certify that Network Design Lab (NDL) Mini Project entitled ***“Cyber Cafe Network”*** Submitted by ***“Krishita Tolia (18104021)”***, ***“Siddhesh Gaikwad (18104069)”*** and ***“Akshata Gawas (18104039)”*** for the partial fulfillment of the requirement for Semester VII Subject of ***Network Design Lab*** in ***BE Information Technology*** to the University of Mumbai, is a bonafide work carried out during Semester VII in Academic Year 2021-2022

Prof. Sonal Jain
Subject Incharge

Prof. Kiran Deshpande
Head Department of Information Technology

External Examiner(s)

1.

Place:A.P.Shah Institute of Technology, Thane

Date:

Declaration

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

(Signature)

(Krishita Tolia 18104021)
(Siddhesh Gaikwad 18104069)
(Akshata Gawas 18104039)

Date:

Introduction

Cyber cafes are widely use networks that helps people to access the internet, avail the internet services, to access the internet information through worldwide, cyber cafes became a dangerous hub that promotes internet crimes, people were using internet to raise terrorism, or hacking bank passwords or card details or any personal details that can harm reputation or status of person in society. Such issues raise the attention of regulation and provision of cyber cafes in India.

Before, people without any authorized permission or prior permission from the government can start their cafes and there is no one to check the mismanagement or inappropriate use of internet in cyber cafes. Cyber cafe means any facility from where access to the internet is offered by any person in the ordinary course of business to the member of the public.

The study on computer networking and technology provides an insight into information into various concepts like the design of topology, IP address configuration and moreover how to send information in form of packets in a single network and secure the user's confidential data from any third party or intruder. In this project, we designed this project in Cisco Packet Tracer using Servers, Routers, Switches, PCs, Laptops, etc and for the connection purposes, we have used the various connecting wires such as copper cables for the best efficiency in network purpose.

Objectives

The main objective of our project:

1. To design a efficient network for cyber cafe.
2. To make the network secure.
3. To modify and enhance the flexibility of network.

Network Requirements

Some of the network requirements are:

1. The network should be scalable.
2. The network should be secure enough for the user.
3. The network should provide proper and fast internet connectivity.

Major Design Areas and Functional Areas

The students must outline the major design areas of a given project topic and identify the functional areas and construct high level modules for it. This project demonstrates the working of Cyber cafe network and allowing remote communication in LAN and allowing usage of Firewall for increasing the security of the network. Also, the network uses EIGRP dynamic routing protocol as scales effectively in a well-designed network, and provides extremely quick convergence times.

Existing Infrastructure

In the existing infrastructure we have PCs in the cybercafé connected to the respective switches. We have an Admin-PC and local server connected to the Cybercafé router. If a user is browsing a website let us say abc.com then it will route from cybercafé router to ISP router to the external router and information would be collected from abc.com server. Elsewhere for security purpose using firewall we have denied access to certain sites.

Network Devices

The Network devices used in the infrastructure includes Routers, switches, PCs and servers. A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets. Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network. A switch has many ports, to which computers are plugged in. A server is a computer or system that provides resources, data, services, or programs to other computers, known as clients, over a network. In theory, whenever computers share resources with client machines they are considered servers.

Request for Proposal (RFP)

Serial no.	Network Devices	Price per Unit	Quantity	Total cost
1	Cisco Switches	17,999	5	89,995
2	Routers	9900	3	29,700
3	Wires	25,000	—	—

Remote Site Connectivity

The students must identify the technology for Remote Site connectivity and evaluate it as per the application requirements of the college campus enterprise network.

IP addressing Plan

In this project, we have achieved dynamic IP addressing i.e. Dynamic Host Configuration Protocol. It is achieved on Internet Protocol networks and automatically assigns an IP addresses to the devices connected to the network. We have created four subnets that are enlisted below:

1. Network: 192.168.0.0/27

Broadcast: 192.168.0.31

HostMin: 192.168.0.1

HostMax: 192.168.0.30

2. Network: 192.168.0.32/27

Broadcast: 192.168.0.63

HostMin: 192.168.0.33

HostMax: 192.168.0.62

3. Network: 192.168.0.64/27

Broadcast: 192.168.0.95

HostMin: 192.168.0.65

HostMax: 192.168.0.94

4. Network: 192.168.0.96/27

Broadcast: 192.168.0.127

HostMin: 192.168.0.97

HostMax: 192.168.0.126

These subnets are used for the dynamic IP assigning for the devices in the Cyber cafe network. A server for Cyber cafe is also installed having IP address 192.168.200.1 along with a host PC having IP address 10.0.0.2. Other external routers are used to demonstrate the real-life working of the network.

Routing Protocol Plan

```
Router>
Router>en
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet6/0
C    20.0.0.0/8 is directly connected, Serial2/0
D    30.0.0.0/8 [90/21024000] via 20.0.0.2, 00:12:11, Serial2/0
D    192.168.0.0/24 is variably subnetted, 3 subnets, 2 masks
D    192.168.0.0/24 is a summary, 00:12:21, Null0
C    192.168.0.0/27 is directly connected, FastEthernet0/0
C    192.168.0.32/27 is directly connected, FastEthernet1/0
C    192.168.200.0/24 is directly connected, FastEthernet7/0

Router#|
```

Figure 1: Cyber Cafe Router

```

Router>en
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

D    10.0.0.0/8 [90/20514560] via 20.0.0.1, 00:13:15, Serial2/0
C    20.0.0.0/8 is directly connected, Serial2/0
C    30.0.0.0/8 is directly connected, Serial3/0
D    192.168.0.0/24 [90/20514560] via 20.0.0.1, 00:13:15, Serial2/0

Router#

```

Figure 2: ISP Router

```

Router>en
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

D    10.0.0.0/8 [90/21026560] via 30.0.0.1, 00:13:50, Serial3/0
D    20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D    20.0.0.0/8 is a summary, 00:13:53, Null0
C    20.10.0.0/24 is directly connected, FastEthernet1/0
C    30.0.0.0/8 is directly connected, Serial3/0
D    192.168.0.0/24 [90/21026560] via 30.0.0.1, 00:13:50, Serial3/0
C    192.168.10.0/24 is directly connected, FastEthernet0/0

Router#

```

Figure 3: External Router

Network Design (Topology Created)

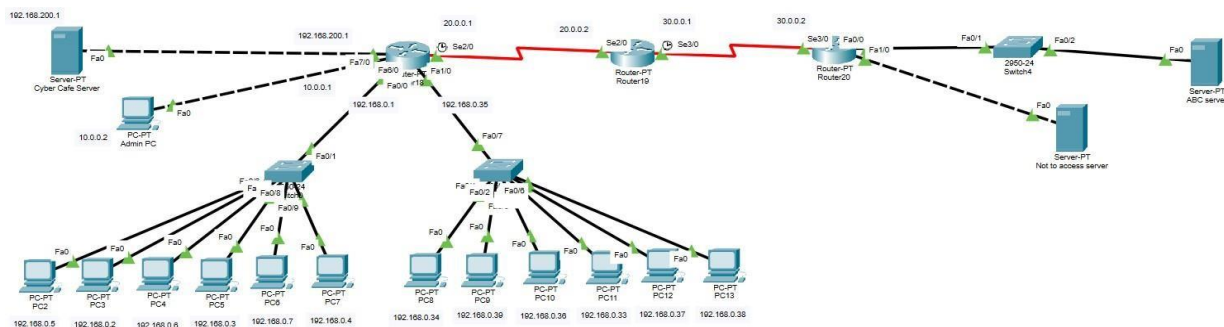


Figure 4: Network Design

Summary

This is the topology for cybercafe. We have performed subnetting with the starting IP address 192.168.0.0. There are four subnets from which two are in use and other two are for future use. We have configured DHCP server, FTP server and also implemented EIGRP routing protocol. Elsewhere for security purpose using firewall we have denied access to certain sites.

References

- [1] Azeez Paul, Chong Zang, "Evaluate Security on the Internet Cafe", Thesis · February 2013 University of Halmstad.
- [2] Alfred Thaga Kgopa, Prof. Ray M Kekwaletswe, "Implementations of Network Security in the Internet Cafés around Pretoria, South Africa" , International Journal of Computer Science and Electronics Engineering (IJCSEE) Volume 2, Issue 1 (2014) ISSN 2320 -401X; EISSN2320-4028.