NETWORK DESIGN PROPOSAL FOR INTERNET CAFE

A COURSE PROJECT REPORT

By

SHUBHAM MAHAJAN (RA2011003011343)
SHANVI KAYAL (RA2011003011344)
PRANSHUL VERMA (RA2011003011361)
SUDHANSHU MAKWANA (RA2011003011365)

Under the guidance of

Mr. NAS Vinoth

In partial fulfillment for the Course

of

18CSC302J - COMPUTER NETWORKS

in Computer Science and Engineering

FACULTY OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

Kattankulathur, Chengalpattu District

NOVEMBER 2022

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Under Section 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that this mini project report "**NETWORK DESIGN PROPOSAL FOR INTERNET CAFE**" is the bonafide work of **Shubham Mahajan (RA2011003011343), Shanvi Kayal (RA2011003011344), Pranshul Verma (RA2011003011361)** and **Sudhanshu Makwana (RA2011003011365)** who carried out the project work under my supervision.

SIGNATURE

MR N.A.S VINOTH
Assistant Professor
CTECH
SRM Institute of Science and Technology

ABSTRACT

This project presents a design and prototype implementation of a cybercafé to support 30 users who all share the same ADSL network, where the access to certain sites(servers) are blocked with the help of a firewall. The café has a printing facility too. A wireless network (ADSL connection) has to be designed that gives users access to certain sites. There are 31 Client computers and a printer to print the files. Three servers are used in the ADSL side to show the working of these computers. The DNS server, the server for Google and YouTube. The IP for YouTube is blocked with the help of a firewall. All 30 PCs are configured to share the same network. A billing software like True café will be installed in all PCs. A common cloud storage will also be used for users to download and print files. This common shared storage avoids cluttering of the PCs' local storage with unnecessary data and the need to manually clean them out after every use.

ACKNOWLEDGEMENT

We express our heartfelt thanks to our honorable **Vice Chancellor Dr. C. MUTHAMIZHCHELVAN**, for being the beacon in all our endeavors.

We would like to express my warmth of gratitude to our **Registrar Dr. S. Ponnusamy,** for his encouragement

We express our profound gratitude to our **Dean (College of Engineering and Technology) Dr. T. V.Gopal,** for bringing out novelty in all executions.

We would like to express my heartfelt thanks to Chairperson, School of Computing **Dr. Revathi Venkataraman,** for imparting confidence to complete my course project

We wish to express my sincere thanks to **Course Audit Professor Dr.Annapurani Panaiyappan, Professor and Head, Department of Networking and Communications** and **Course Coordinators** for their constant encouragement and support.

We are highly thankful to our my Course project Faculty **MR N.A.S VINOTH , Assistant Professor , TECH,** for his/her assistance, timely suggestion and guidance throughout the duration of this course project.

We extend my gratitude to our **HoD Dr Pushplata ,CTECH** and my Departmental colleagues for their Support.

Finally, we thank our parents and friends near and dear ones who directly and indirectly contributed to the successful completion of our project. Above all, I thank the almighty for showering his blessings on me to complete my Course project.

TABLE OF CONTENTS

1. INTRODUCTION

WIRELESS NETWORK

Admin telecommunications networks are normally introduced and administered using radio communication. This exercise takes place at the physical level of OSI (layer)
The first technical wireless network was established under the brand ALOHAnet at the University of Hawaii in 1969 and became operational in June 1971. The first commercial wireless network was the WaveLAN family of products developed by NCR in 1986.

ROUTERS

The concept of an Interface computer was first proposed by Donald Davies for the NPL network in 1966. The same idea was conceived by Wesley Clark the following year for use in the ARPANET. Named Interface Message Processors (IMPs), these computers had fundamentally the same functionality as a router does today. The idea for a router (called gateways at the time) initially came about through an international group of computer networking researchers called the International Networking Working Group (INWG). Set up in 1972 as an informal group to consider the technical issues involved in connecting different networks, it became a subcommittee of the International Federation for Information Processing later that year. These gateway devices were different from most previous packet switching schemes in two ways. First, they connected dissimilar kinds of networks, such as serial lines and local area networks. Second, they were connectionless devices, which had no role in ensuring that traffic was delivered reliably, leaving that entirely to the hosts. This particular idea, the end-to-end principle, had been previously pioneered in the CYCLADES network.

SWITCH

A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer (layer 2) of the OSI model. Some switches can also forward data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.
Switches for Ethernet are the most common form of network switch. The first Ethernet switch was introduced by Kalpana in 1990.
Switches also exist for other types of networks including Fibre Channel, Asynchronous Transfer Mode, and InfiniBand.

ADSL

ADSL was specifically designed to exploit the one-way nature of most multimedia communication in which large amounts of information flow toward the user and only a small amount of interactive control information is returned. Several experiments with ADSL to real users began in 1996. In 1998, wide-scale installations began in several parts of the U.S. In 2000 and beyond, ADSL and other forms of DSL are expected to become generally available in urban areas. With ADSL (and other forms of DSL), telephone companies are competing with cable companies and their cable modem services.

Ethernet

Ethernet was developed at Xerox PARC between 1973 and 1974. It was inspired by ALOHAnet, which Robert Metcalfe had studied as part of his PhD dissertation. The idea was first documented in a memo that Metcalfe wrote on May 22, 1973, where he named it after the luminiferous aether once postulated to exist as an "omnipresent, completely-passive medium for the propagation of electromagnetic waves." In 1975, Xerox filed a patent application listing Metcalfe, David Boggs, Chuck Thacker, and Butler Lampson as inventors. In 1976, after the system was deployed at PARC, Metcalfe and Boggs published a seminal paper. Yogen Dalal, Ron Crane, Bob Garner, and Roy Ogus facilitated the upgrade from the original
2.94 Mbit/s protocol to the 10 Mbit/s protocol, which was released to the market in 1980.

2. REQUIREMENTS

2.1 Network design requirement

To design a network for an internet café which has 30 users. The internet café has one ADSL which is to be shared among the users. Certain websites must be blocked on all computers in the café. A café billing management system must be configured and deployed in the café.

2.2 Problems faced

PHYSICAL

1. Cluster of wires- the WAN network of wires requires a good amount of wiring, so it should be properly managed.
2. Printer Management- as there are only three printers, customers will have to wait to use them.
3. Speed- laying high quality wires (Optical Fiber) is necessary for a WAN network else the reception of data will be slowed down.
4. Complexity- the model is a bit complicated but efficient. Care should be taken while making the connections between various devices.

TECHNICAL

1. Loss of internet access and packets.
2. Lack of ability to print.
3. Security of the PC and data associated.
4. Common storage has to be cleaned out on a daily basis.
5. Billing software must be up to date and accurate.
6. Low or Insufficient bandwidth may result in slowed down results and functioning.

2.3 Objectives

1. Proper and careful management of clusters of wires.
2. Check proper functioning of all devices on a regular basis.
3. Use high quality materials to ensure the quality remains up to the mark.
4. Use of firewall to ensure the security of the incoming and outgoing data.
5. Using the most efficient layout of devices.
6. Properly calibrated switches.

2.4 Design Requirement Analysis

The internet café is to support 30 users. So, 30 Desktop computers would be required. For the local network of computers, a switch would be required. Since 30 computers need to be networked, a switch with 30 ports would be required. Switches typically come with 24 ports or 48 ports. Since a 24-port switch would not suffice the requirement, a 48-port switch is recommended. But in our implementation, to make the design more efficient we use two switches each with 24 ports, and 15 computers are connected to the first switch and 16 computers, and 3 printers to the second one.

An ADSL router which is capable of NAT (Network Address) is required. NAT is a mandatory feature which is required on the router, for sharing the ADSL internet connection.

Although not mandatory, a DHCP server is preferred for providing dynamic IP addresses to the users. The availability of the feature on the router rules out the need to setup and configure an additional DHCP server for this network
In our scenario, we use a firewall coupled with the DSL router-modem, with the configurations made directly within the former.

An ISP router is responsible for connecting all the PC's to the internet.

Three servers are used in this implementation, one server for the DNS, and the rest two being that of Google and YouTube, where the google server is accessible by all the 30 PC's and the access of the site youtube.com is prohibited by the café's guidelines.

As the users in the café need to be managed with a billing system, additional software must be installed and configured on the appropriate operating system for which it is supported. Here we would use software like TrueCafe which is usually installed on the admin computer and rolled out to the other users.

2.5 Hardware Required

1) ADSL and ISP Router
2) 3 Switches
3) 31 Client Computers
4) 3 Printers
5) 1 Firewall
6) 3 Servers
7) 1 Modem
8) 1 Cloud Service

2.6 Specifications

Router 2811(NM-ESW-161 port) and Router 1841

The Cisco 1841 router is designed for secure data connectivity and provides significant additional value compared to prior generations of Cisco 1700 Series routers by offering more than a fivefold performance increase and integrated hardware-based encryption enabled by an optional Cisco IOS ® Software security image. The Cisco 1841 dramatically increased interface card slot performance and density over the Cisco 1700 Series while maintaining support for more than 30 existing WAN interface cards (WICs) and multiflex trunk cards.

2960-24TT Switches

Cisco Catalyst 2960 Series Switches with LAN Lite software are fixed-configuration, standalone switches that provide desktop Fast Ethernet connectivity for entry-level wiring closet and small branch-office networks . These switches simplify the migration from non-intelligent hubs and unmanaged switches to a fully scalable managed network. Cisco Catalyst 2960 Series Switches have lower cost of ownership with features such as intelligent switch configuration using Auto Smart Ports, installation with Auto Install and enhanced troubleshooting to facilitate ease of use.

PC-PT Computers

A device that performs processes, calculations and operations based on instructions provided by a software or hardware program. It has the ability to accept data (input), process it, and then produce outputs.

Printer-PT

A Printer is a peripheral device which makes a persistent representation of graphics or text, usually on paper. While most output is human-readable, barcode printers are an example of an expanded use for printers.

Cisco ASA 5505

Cisco ASA 5500 Series Adaptive Security Appliances are purpose- built solutions that integrate world-class firewall, unified communications security, VPN, intrusion prevention (IPS), and content security services in a unified platform.
The Cisco ASA 5500 Series provides intelligent threat defense that stops attacks before they penetrate the network perimeter, controls network and application activity, and delivers secure remote access and site-to-site connectivity. The result is a powerful multifunction network that provides security breadth, precision, and depth for protecting the café network, while reducing the overall deployment and operations costs associated with implementing comprehensive multilayer security.

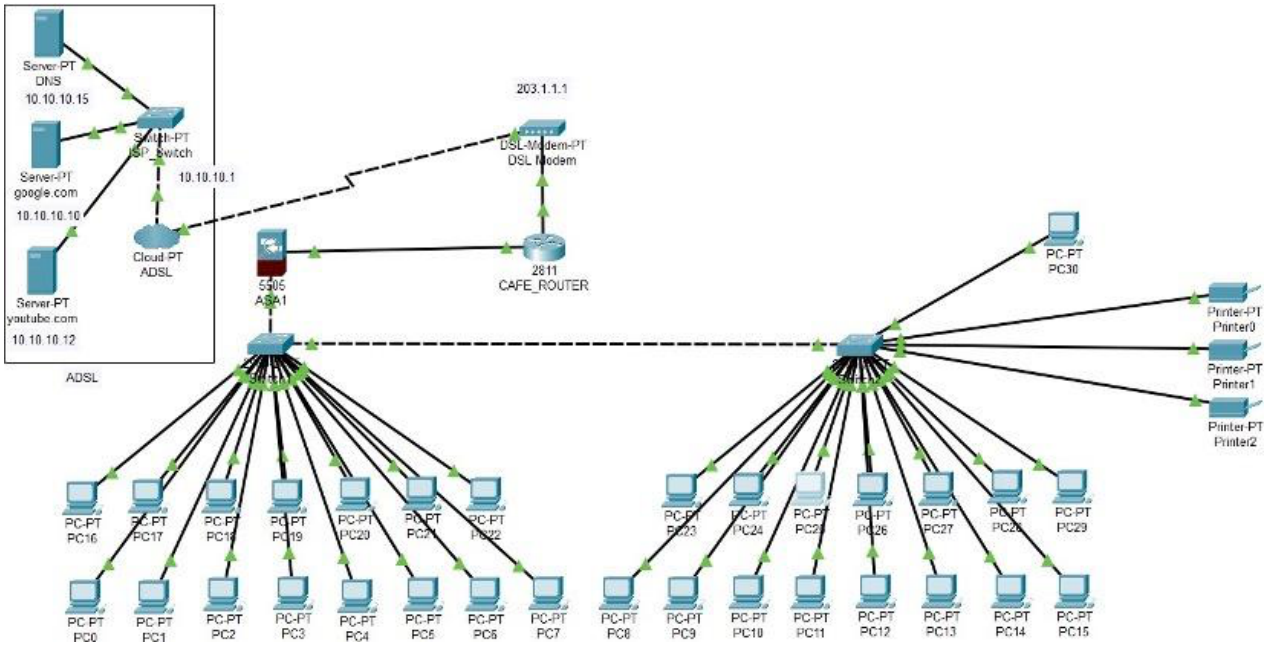
Server-PT servers

Servers are an entirely different breed when compared to other end devices. They have various functionalities and also have space for two network interfaces. The modules available for servers are the same as PC modules, except that the servers do not have the PC- HOST-NM-1AM module.

3. ARCHITECTURE AND DESIGN

3.1 Network Architecture

The network architecture is as follows:



● The computers corresponding to the users connect to the ports on the switches. As Shown in the fig. above.

● The switches are 24 port switches each. The computer connects to the switch using Ethernet RJ 45 cables.

● The café management software is installed on the appropriate operating system and set up on the network.

● The firewall along with the ADSL router-modem is deployed as shown in the diagram. This has two interfaces. The WAN interface of the router is connected to the internet and the LAN interface is switched.

● The ADSL router is configured for NAT. When the feature is enabled, internal users would be able to share the IP Address which would be available on the WAN interface of the router.

● The DHCP feature on the firewall is configured for NAT. When the right command is called, it would provide appropriate IP Address, subnet mask, default gateway and DNS server IP Addresses for the
user's computers.

4. IMPLEMENTATION

4.1 IP Address Implementation

● The internal private IP Address range for the users and other devices within the café is 192.168.1.2-36.

● The subnet masks of all the devices are the same – 255.255.255.0

● The IP Addresses of the LAN interface of the firewall and computer on which the café management system is set up should be configured with static IP Addresses (192.168.10.1) belonging to 192.168.1.0/31.

● It should be ensured that the static IP Addresses provided for the LAN interface of the firewall and the café management system are excluded from the DHCP scope configured on the router for avoiding duplicate IP addressing.

● The default gateway and the DNS server which is to be provided in the DHCP scope would be the IP address of the LAN interface of the firewall.

● The default gateway for the three servers, i.e., the DNS server, Google server and YouTube server, is the same – 10.10.10.1

DNS SERVER

IP = 10.10.10.15
Default Gateway – 10.10.10.1
Port (server to switch) = Fast Ethernet 0 to Fast Ethernet 0/1 of the switch
DNS Service = ON
Resource Records = www.google.com (10.10.10.10)
www.youtube.com (10.10.10.12)

GOOGLE SERVER

IP = 10.10.10.10
Default Gateway – 10.10.10.1
Port (server to switch) = Fast Ethernet 0 to Fast Ethernet 1/1 of the switch
HTTP Service – ON
HTTPS Service – ON

YOUTUBE SERVER

IP = 10.10.10.12
Default Gateway – 10.10.10.1
Port (server to switch) = Fast Ethernet 0 to Fast Ethernet 2/1 of the switch
HTTP Service – ON HTTPS Service – ON

● The switch is connected to Ethernet 6 of the cloud via port Fast Ethernet 3/1 with the help of a Copper Cross-Over.

● The cloud is connected to modem 4 with the help of a Phone cable. The name of the modem and the port used for connection are added under DSL service of the cloud.

● The IP of the interface between the ADSL connection and the café modem is the default gateway used for the servers, i.e., 10.10.10.1

● The IP of the interface between the modem and the router of the café is the default gateway used earlier, i.e., 10.10.10.1. The port used is Fast Ethernet 0/0 of the router.

● The IP of the interface between the router and the firewall device is the default gateway of the router, i.e., 203.1.1.1. The port used is Fast Ethernet 0/1 of the router and Ethernet 0/0 of the firewall.

4.2 Router configuration

Router(config)#interface FastEthernet 0/0 Router(config-if)#ip address 203.1.1.1

255.255.255.0 Router(config-if)#no shutdown

Router(config-if)#exit Router(config)#interface FastEthernet 0/1

Router(config-if)#ip address 10.10.10.1 255.255.255.0 Router(config-if)#no shutdown

Router(config)#router ospf 1

Router(config-router)#network 203.1.1.0 0.0.0.255 area 0

Router(config-router)#network 10.10.10.0 0.0.0.255 area 0

4.3 Cisco ASA 5505 configuration

ciscoasa(config)#interface vlan 1 ciscoasa(config-if)#no ip address

ciscoasa(config)#no dhcpd address 192.168.1.5-192.168.1.35 inside

ciscoasa(config)#interface vlan 1

ciscoasa(config-if)#ip address 192.168.10.1 255.255.255.0 ciscoasa(config-if)#no shutdown

ciscoasa(config-if)#nameif inside ciscoasa(config-if)#security-level 100

ciscoasa(config-if)#exit ciscoasa(config)#interface vlan 2

ciscoasa(config-if)#ip address 203.1.1.2 255.255.255.0 ciscoasa(config-if)#no shutdown

ciscoasa(config-if)#nameif outside ciscoasa(config-if)#security-level 0

ciscoasa(config-if)#exit ciscoasa(config)#interface ethernet 0/1 ciscoasa(config-if)#switchport access vlan 1 ciscoasa(config)#interface ethernet 0/0 ciscoasa(config-if)#switchport access vlan 2 ciscoasa(config-if)#exit

ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 203.1.1.1 ciscoasa(config)#object network LAN

ciscoasa(config-network-object)#subnet 192.168.10.0 255.255.255.0

ciscoasa(config-network-object)#nat (inside,outside) dynamic interface

ciscoasa(config-network-object)#exit

ciscoasa(config)#access-list al extended deny ip 10.10.10.12 0.0.0.255 any

ciscoasa(config)#access-list al extended permit tcp any any ciscoasa(config)#access-list al extended permit icmp any any ciscoasa(config)#access-group al in interface outside

● The firewall is connected to the first switch via port FastEthernet 0/17.

● The default gateways of all the 31 PCs and the printers is the IP used at the interface for the firewall, i.e, 192.168.10.1.

● All the PCs are connected to the switches via their port Fa0.

● The first switch is connected to the second via ports Fa0/1 and Fa0/18 of the first and second switch respectively.

4.4 IP Address Configuration

IP configurations of the PCs along with the port of the switch they are connected to:

PC0:
IPv4 address = 192.168.10.36
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/3

PC1:
IPv4 address = 192.168.10.5
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/5

PC2:
IPv4 address = 192.168.10.5
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/5

PC3:
IPv4 address = 192.168.10.9
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/9

PC4:
IPv4 address = 192.168.10.11
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/11

PC5:
IPv4 address = 192.168.10.13
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/13

PC6:
IPv4 address = 192.168.10.15
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/15

PC7:
IPv4 address = 192.168.10.16
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/16

PC8:
IPv4 address = 192.168.10.18
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/1

PC9:
IPv4 address = 192.168.10.20
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/3

PC10:
IPv4 address = 192.168.10.22
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/5

PC11:
IPv4 address = 192.168.10.24
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/12

PC12:
IPv4 address = 192.168.10.26
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/13

PC13:
IPv4 address = 192.168.10.28
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/14

PC14:
IPv4 address = 192.168.10.30
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/15

PC15:
IPv4 address = 192.168.10.32
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/16

PC16:
IPv4 address = 192.168.10.17
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/2

PC17:
IPv4 address = 192.168.10.4
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/4

PC18:
IPv4 address = 192.168.10.6
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/6

PC19:
IPv4 address = 192.168.10.8
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/8

PC20:
IPv4 address = 192.168.10.10
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/13

PC21:
IPv4 address = 192.168.10.12
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/12

PC22:
IPv4 address = 192.168.10.14
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/14

PC23:
IPv4 address = 192.168.10.19
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/2

PC24:
IPv4 address = 192.168.10.21
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/4

PC25:
IPv4 address = 192.168.10.23
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/6

PC26:
IPv4 address = 192.168.10.25
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/13

PC27:
IPv4 address = 192.168.10.27
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/15

PC28:
IPv4 address = 192.168.10.29
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/9

PC29:
IPv4 address = 192.168.10.31
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/10

PC30:
IPv4 address = 192.168.10.33
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/11

Printer0:
IPv4 address = 192.168.10.34
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/17

Printer1:
IPv4 address = 192.168.10.35
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/19

Printer2:
IPv4 address = 192.168.10.37
Subnet mask = 255.255.255.0
Default gateway = 192.168.10.1
DNS Server = 10.10.10.15
Port = Fa 0/20

5. INFERENCE

A network design for an internet cafe supporting 30 users has been created successfully. All users share a common ADSL network. Certain websites have been blocked using an extended ACL in the firewall. A billing software has been installed on all the PCs to monitor usage. The cafe also has printing, FAX and Xerox facilities. The PCs are coupled with a common storage for the users to download and print files.

All the possible issues have been considered and suitable measures have been taken to avoid them. The devices have been configured and a working model of the network has been created on a simulator (Cisco Packet Tracer) successfully.

6. REFERENCES

1. https://www.wikipedia.org
2. https://www.cisco.com/c/dam/en_us/training-events/netacad/course_catalog/docs/Cisco_PacketTracer_DS.pdf
3. Kurose, J.F. and K.W. Ross (2003) *Computer Networking: A Top Down Approach Featuring the Internet*, Addison Wesley.
4. Mir, N.F. (2006) *Computer and Communication Networks*, Prentice Hall.
5. Tanenbaum, A.S. (2002) *Computer Networks*, Prentice Hall.
6. https://curlie.org/Computers/Software/Networking/
7. Behrouz A. Forouzan, "TCP IP Protocol Suite " 4th edition, 2010, McGraw-Hill ISBN: 0073376043.
8. Douglas E. Comer, Internetworking with TCP/IP, Principles, protocols, and architecture, Vol 1 5th Edition,2006 ISBN: 0131876716, ISBN: 978-0131876712.
9. Richard Stevens, Unix Network Programming, vol.1, 3rd edition, 2003, McGraw-Hill ISBN 0-07-246060.