A Mini Project Report

On

Network Design for Internet Cafe

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

Network Design Lab

In

Information Technology

by

Rupal Sonje 18IT1086

Riteshkumar Singh 18IT1068

Soham Salkar 18IT1050

Subject In-Charge
Mrs. Nilima Dongre

Department of Information Technology

Dr. D. Y. Patil Group's

Ramrao Adik Institute Of Technology

Dr. D. Y. Patil Vidyanagar, Sector 7, Nerul, Navi Mumbai 400706.

(Affiliated to University of Mumbai)

2021-2022

Ramrao Adik Institute of Technology

(Affiliated to the University of Mumbai)

Dr. D. Y. Patil Vidyanagar,Sector 7, Nerul, Navi Mumbai 400706.

CERTIFICATE

This is to certify that, the Mini Project titled

“Network Design for Internet Cafe”

is a bonafide work done by

Rupal Sonje Roll No. 18IT1086

Riteshkumar Singh Roll No. 18IT1068

Soham Salkar Roll No. 18IT1050

Subject In-Charge

Mr. Nilima Dongre

Head of Department

(Dr. Ashish Jadhav)

External Examiner

Date : 27/10/2021

Declaration

We declare that this written submission represents our ideas in our own words and where other's 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 falsi- fied any idea/data/fact/source in our 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.

Sonje	Ritesh	
Rupal Sonje	Riteshkumar Singh	Soham Salkar
(18IT1086)	(18IT1068)	(18IT1050)

Date : 27/10/2021

Abstract

The main aim of the project is to design a suitable network system for the Internet Cafe. We are focusing on considering a network design for an area with one head office and three sub branches. This project will provide a backup of data and security to the network with minimum cost and proper bandwidth utilization. There are many devices that were used in designing the network, such as routers, switches, iot devices like printers and webcam, routing protocols and servers. All of these utilities have been configured to provide a secure environment for the entire network and to prevent hackers from accessing sensitive information. Improving the performance of any network requires a high quality of techniques and services which help to improve the general task of the network.

TABLE OF CONTENTS

LIST OF FIGURES

1. Introduction

Stable, high-speed and secure wireless network is the basic standard for the Internet cafe to provide convenient access to services to its customers as well as workers. It is argued that Internet usage is likely to increase due to the increasing availability of network infrastructures, faster connection speeds, and lower connection costs in terms of Internet technologies. Most businesses today have systems that also operate on the Internet for customer self-services.

Internet cafés are increasingly providing Internet opportunities for ordinary people who can’t afford to have Internet access at their homes. Many people use the Internet café to access their webmail, engage in instant messaging, to keep in touch with friends and families via social networks such as Facebook, Twitter, and other social network media. Apart from engaging in social networks, many also go to Internet cafés to perform different actions such as online research, accessing online systems to perform their business transactions, while others use it to do their online banking and shopping.

The main factors considered for designing the network are: adaptability, integration, security and cost. This design has focused on a low cost, high security level network for the internet cafe to cut down their expenses and provide their customers with better performance and customer satisfaction.

2. Objectives

The main objectives of this project is to demonstrate an example of a internet cafe network design that:

- The system aims to improve
    - monitoring
    - control over rental computers.
- Provides a high level security and backup for the data.
- Maintains a low cost and efficient performance.
- Provides flexible deployment and convenient management.
- Provides an efficient performance to the customers as well as workers of the company.

3. Network Requirements

Fundamental Design Goals

When examined carefully, these requirements translate into four fundamental network design goals:

- **Scalability**: Scalable network designs can grow to include new user groups and remote sites and can support new applications without impacting the level of service delivered to existing users.
- **Availability**: A network designed for availability is one that delivers consistent, reliable performance. In addition, the failure of a single link or piece of equipment should not significantly impact network performance.
- **Security**: Security is a feature that must be designed into the network, not added on after the network is complete. Planning the location of security devices and filters are critical to safeguarding network resources.
- **Manageability** : No matter how good the initial network design is, the available network staff must be able to manage and support the network. A network that is too complex or difficult to maintain cannot function effectively and efficiently.

The hardware and software requirements which we need in our project are:

1. Windows 10/ Windows 7/ Windows 8 platform
2. Packet tracer (MAN, LAN, VLAN, ACL, VPN)
3. Routers
4. Multilayer switches
5. Switches
6. Servers (DHCP,DNS,WEB SERVER,SMTP)
7. PCs
8. Printer(various wired devices)
9. Usable protocols: RIP (Routing Information Protocol)
10. Webcam
11. Cabling

4. Major Design Areas and Functional Areas

Major Design Areas The following are the major design areas to be addressed:

Redesign the campus LAN: The current campus LAN is shared and inter connects four branches. Because there is no redundancy, the designer needs to entirely redesign the campus, including the placement of servers.

Redesign the IP addressing scheme: The flat addressing scheme and static routes are not desirable features in a scalable growing network. New hierarchical addressing is required.

Introduce a new routing protocol: The internet cafe is aware of the drawbacks of static routes. The designer should implement a dynamic routing protocol that is more scalable and that better fits the planned hierarchical addressing scheme.

Upgrade the WAN links: The upgrade of the WAN links is essential because, according to the internet cafe, the current bandwidth seems insufficient. The introduction of new applications along with the existing applications will result in a higher load on the WAN links.

Enterprise Architecture of Cisco to the Internet Cafe network requirements and develop a high level view of the planned network hierarchy. Consider each of the functional areas of the Cisco Enterprise Architecture:

- Enterprise Campus : Including the Campus Infrastructure module composed of the Campus Core Layer, Distribution Layer, Access layer and the server farm module.
- Enterprise Edge: WAN, MAN, and site to site VPN module
- Enterprise Branch
- Enterprise Data Centre
- Enterprise Teleworker

Key considerations of functions for each of the modules in

Enterprise Campus Building Access Layer:

- Each branch has a building access layer.
- This layer supports important services such as broadcast suppression, protocol filtering, network access, IP Multicast, and QoS. Layer 2 functions as VLANs and spanning trees are also provided by this layer.
- For high availability the access layer switches could be dual attached to the distribution layer switches.

Enterprise Campus Building Distribution Layer:

- Main branch has a Building Distribution Layer, which could be combined 8 with the campus core in the main branch.
- This layer aggregates access networks using multilayer switching and performs routing, QoS and access control.
- Redundancy and load balancing with both the access and core layers is recommended.

Enterprise Campus Core Layer:

- This layer provides redundant and fast-converging connectivity between branches and with the server farm and enterprise edge modules, routing and switching traffic as fast as possible from one module to another.
- This layer uses multilayer switches for high throughput.

Enterprise Server Farm Module:

- This layer contains internal e-mail and corporate servers that provide Application, file, print, e-mail, and DNS services to internal users.
- Because access to these servers is vital, as a best practice they should be connected to two different switches, enabling full redundancy and load sharing.

Enterprise Branch: This module allows branch office users to connect to the central site to access company information. Therefore, it benefits from high-speed internet access, VPN connectivity to corporate intranets, video Conferencing, meetings and fax calls over the managed IP networks.

Additional modules required :

For managing the huge data of customers and sharing it over the servers. Internet connectivity module, an E-commerce module, a remote access module and possibly an Enterprise teleworker module will be added to the network design.

Network Services applicable to Internet Cafe design:

1.Security Services- The customer data in the cafe is confidential and an intruder must not tamper or steal the data. Thus security services should support the internet connectivity, E-commerce, and Remote access and IDS must be proper.

2. High Availability- High availability is needed in WAN as the user might require access to his services.

Indicate where redundancy should be supported in design :

Redundancy in the Enterprise Campus is most critical in the campus core layer, followed by the Building distribution layer. As redundancy helps in delivering high productivity and customer satisfaction even with low bandwidth network connectivity. The WAN router could be made redundant.

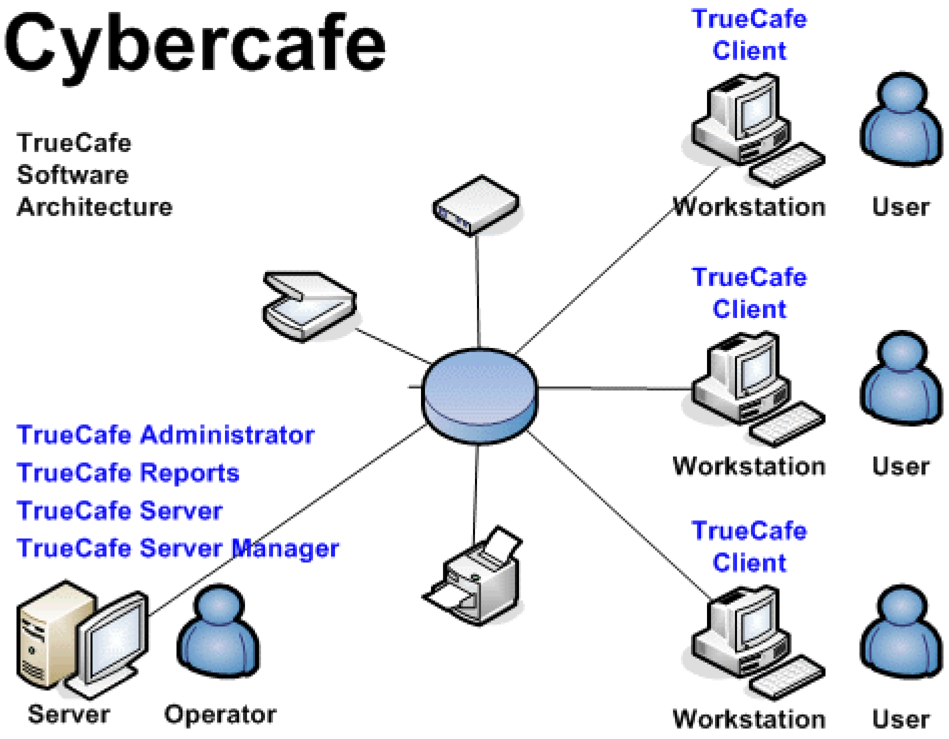


Fig 4.1 Cyber Cafe Network

5. Infrastructure

It will be always efficient to follow the structured cabling approach in designing a network. Structured cabling is made up of a number of standardized elements called subsystems. The subsystems are entrance facility where ISP network ends and connects to customer devices, equipment room where several equipment and other parts of network that serve the clients inside the building, backbone cabling which interconnects different floors together with high speed cables, horizontal cabling which interconnects the components inside the same floor, work area where the end user equipment connect together with horizontal cabling and telecommunication enclosure which interconnects horizontal cabling and backbone cabling together. So, in this network design also structured cabling approach is followed. Work area subsystem consists of several end user workstations which are connected to the wall socket through RJ45 cables. Work area also includes a wireless station communicating with the nearest access point (AP). Horizontal cabling in this network design is made up of 100Mb/s Ethernet cables (Twisted Pair – CAT5) which joins the wall sockets (terminating point of wired workstations) and the back pane of patch panel. Telecommunication enclosure subsystem in this network design consists of switch chassis and patch panels. Patch panel wires (Patch cords) are used to connect the front end of patch panel and individual switch (switch ports) in the switch chassis.

The reasons to use patch panel in this network design are:

- Identification – Ports in patch panel can be labelled, to uniquely identify which cable comes from which location is getting terminated on which port of patch panel. So, it is easy to disconnect/connect and testing a cable.

- Small changes in network cabling would not affect the switches in switch chassis. So, changes can be made quickly and easily.

- All the cables can be terminated on the patch panels (irrespective of whether they need to be connected to the switches or not) and they could be selectively connected to the switches by just moving the patch cables, whenever needed.

- Network maintenance becomes easy. In the stack, each switch acts as a single unit, so there is a single management interface thus simplifies the operation and configuration of the network.

- Scalability – The network can grow by additional switches over the time when needed, thus reducing management complexity.

- Even if one unit (switch) fails, data will continue to flow through other units, thus provides resilient connections.

- Switches can function as stackable switches (operate together as a single unit), or they can be configured to operate independently, thus providing deployment flexibility.

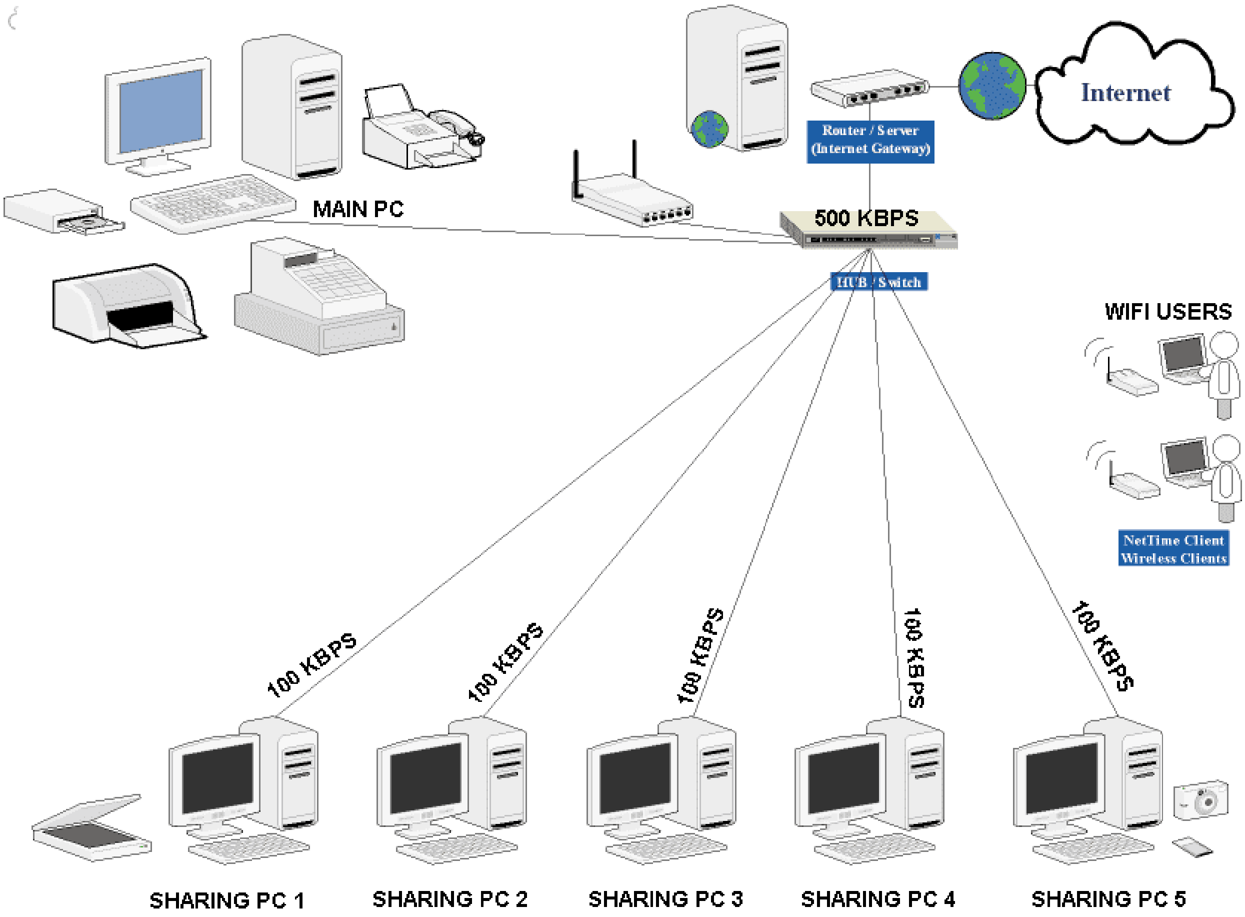


Fig 5.1 Existing System

6. Network Devices

Phase 1 – Designing the network

No of machines the Internet Cafes network can support: 40 users in each branch office and 80 users in main office Type of network media used:

- Ethernet / FDDI (LAN)
- Copper Media / Fiber Optic Media / wireless (WANs)

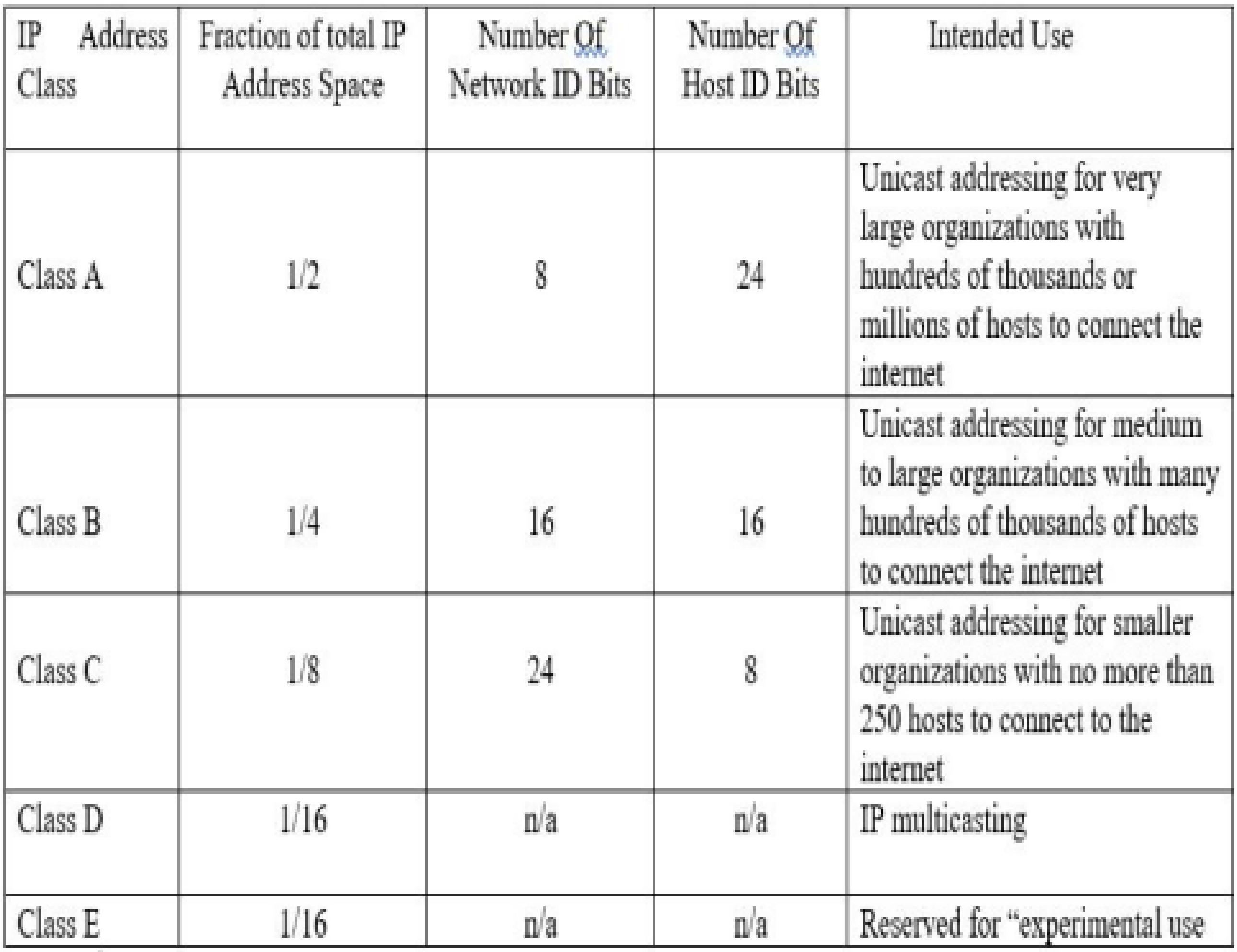
Network topology:

- Star/Mesh Topology configured in wireless Networks

Phase 2 – Setting up an IP Addressing Scheme

Network class applied : IPv4

Reasons why IPv4 is chosen:



IP Address Class	Fraction of total IP Address Space	Number Of Network ID Bits	Number Of Host ID Bits	Intended Use
Class A	1/2	8	24	Unicast addressing for very large organizations with hundreds of thousands or millions of hosts to connect the internet
Class B	1/4	16	16	Unicast addressing for medium to large organizations with many hundreds of thousands of hosts to connect the internet
Class C	1/8	24	8	Unicast addressing for smaller organizations with no more than 250 hosts to connect to the internet
Class D	1/16	n/a	n/a	IP multicasting
Class E	1/16	n/a	n/a	Reserved for "experimental use

• IPv4 still carries more than 96 percent of internet traffic worldwide as of May 2014

• Take the potential transition from IPv4 into IPv6 in the future into consideration.

Phase3 – Naming Entities on the Internet Cafe Network

• Names assigned are used for initial set up in the network
• For expanding the network through routers or PPP (Point to point protocols)

• Easier for users to identify the machines and servers in the network.

Name Service selected : DNS (Domain Name System)

• Anti-phishing and anti – spam mechanism at application server. • Privacy mechanism helps hide internal network topology.

Network devices required for Internet Cafe Server include :

- DHCP Server
- Surveillance camera
- Printer
- Router

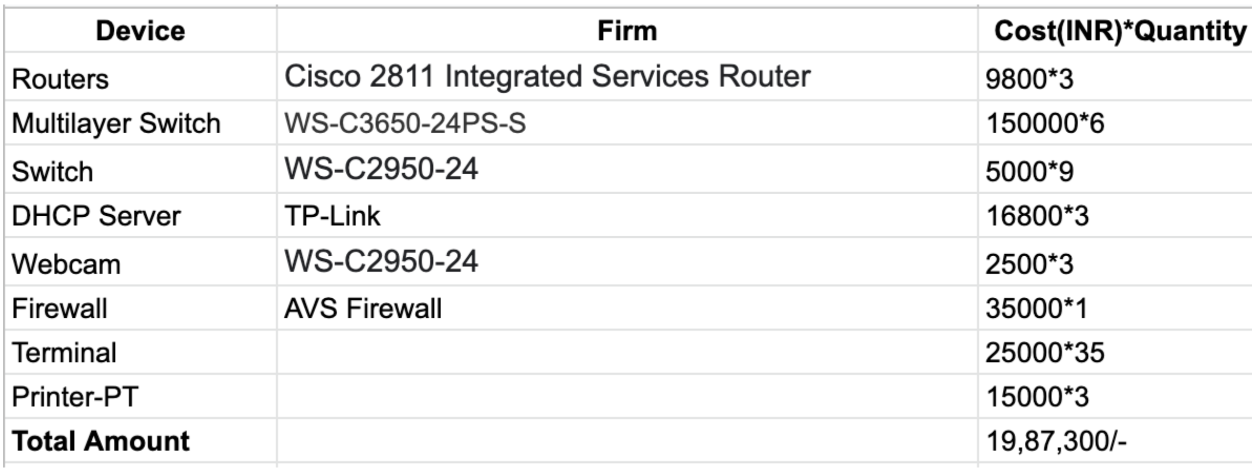
Management and board remain in control of the content, performance, and security.

7. Request For Proposal(RFP)

Cost Estimation: Total approximate cost required to connect three branches to a main branch of an Internet Cafe is estimated below.

The most logical choice would be to use twisted pair cable, as twisted pair cable is the customary choice for local area network (LAN). Often abbreviated as UTP for the unshielded twisted pair, UTP is composed of eight wires that have been twisted into four pairs. The category of cable that will be used for this network design is CAT-5e. The CAT-5e is rated to 350 Mhz. CAT-5e has 100- ohm impedance and electrical attributes supporting transmissions up to 100 MHz.

Table of total cost required to build the network:



Device	Firm	Cost(INR)*Quantity
Routers	Cisco 2811 Integrated Services Router	9800*3
Multilayer Switch	WS-C3650-24PS-S	150000*6
Switch	WS-C2950-24	5000*9
DHCP Server	TP-Link	16800*3
Webcam	WS-C2950-24	2500*3
Firewall	AVS Firewall	35000*1
Terminal		25000*35
Printer-PT		15000*3
Total Amount		19,87,300/-

8. Remote Site Connectivity

Multiple remote-site WAN designs are based on various combinations of WAN transports mapped to the site specific requirements for service levels and redundancy. The remote-site designs include single or dual WAN edge routers. These can be either a CE router or a VPN spoke router. In some cases, a single WAN edge router can perform the role of both a CE router and VPN-spoke router. Most remote sites are designed with a single router WAN edge; however, certain remote site types require a dual router WAN edge. Dual router candidate sites include regional office or remote campus locations with large user populations, or sites with mission-critical needs that justify additional redundancy to remove single points of failure. The overall WAN design methodology is based on a primary WAN aggregation site design that can accommodate all of the remote-site types that map to the various link combinations listed in Table:

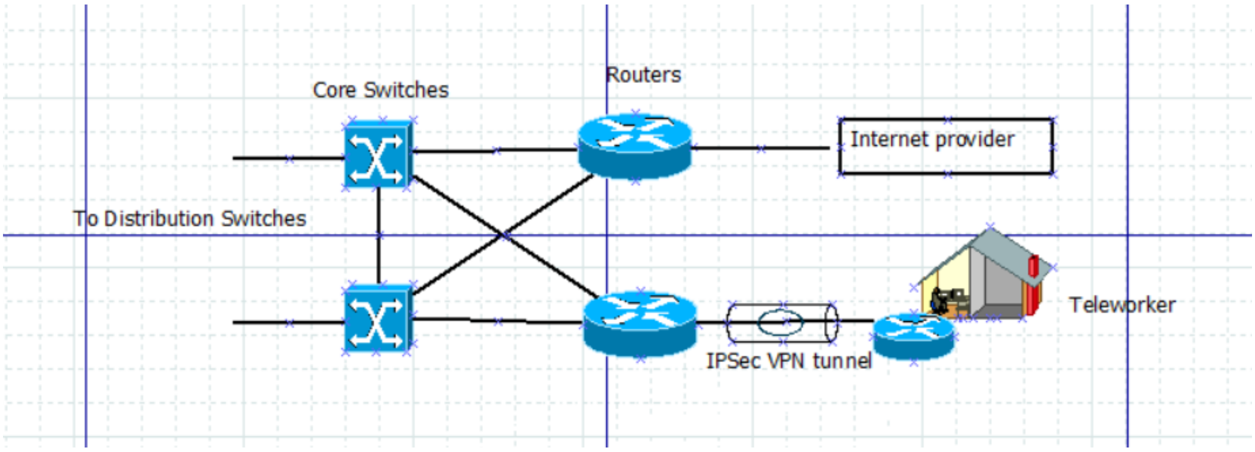


Fig 8.1 Internet Cafe Network Structure

The LAN is the networking infrastructure that provides access to network communication services and resources for end users and devices spread over a single floor or building. You create a campus network by interconnecting a group of LANs that are spread over a small geographic area. Campus network design concepts are inclusive of small networks that use a single LAN switch, up to very large networks with thousands of connections. The campus wired LAN enables communications between devices in a building or group of buildings, as well as interconnection to the WAN and Internet edge at the network core. Specifically, this design provides a network foundation and services that enable:

- Tiered LAN connectivity.
- Wired network access for employees.
- IP Multicast for efficient data distribution.
- Wired infrastructure ready for multimedia services.

A hierarchical LAN design includes the following three layers: • Access layer—Provides endpoints and users direct access to the network. • Distribution layer—Aggregates access layers and provides connectivity to services.

• Core layer—Provides connectivity between distribution layers for large LAN environments.

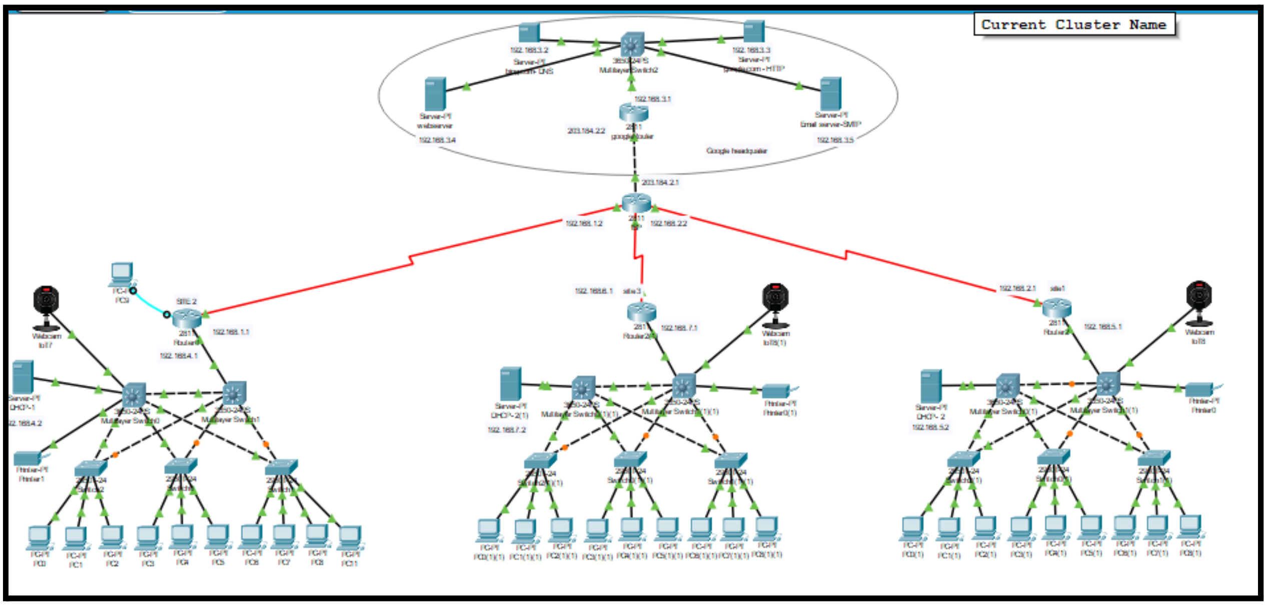


Fig. 8.2: Internet cafe Design

9. IP Addressing Plan

IP addresses of every branch of the Internet Cafe are allocated by DHCP. DHCP is the method that dynamically assigns IP addresses for the client. The server can assign an IP address automatically from the IP address of the preset pool to host. It not only ensures that IP addresses can not be distributed repeatedly, but also recovers IP addresses timely to ensure the utilization of IP addresses. DHCP is scalable and relatively easy to manage. This scheme in the building uses DHCP dynamically assigned IP addresses. Deploying the DHCP pool for each VLAN in layer 3 switches makes VLAN automatically access the address and implement DHCP backup. It not only eliminates the trouble of administrator operation, but also distributes reasonably the IP addresses to each user.

IP Address plan:

Location	IP Address Block
Site 1	192.168.5.1/2 192.168.5.1 - 192.168.5.15
Site 2	192.168.4.1/24 192.168.4.1-192.168.4.15
Site 3	192.168.7.1/24 192.168.7.1-192.168.7.15

10. Routing Protocol Plan

In Internet cafe network design, we will use Full Mesh and Highly redundant designs.

Full Mesh Topologies :

Full mesh topologies are a less common design element in networks, but they are worth considering because the scaling properties of a routing protocol in a full mesh design indicate, to some degree, the scaling properties of the same protocol in a partial tree-mesh design topology.

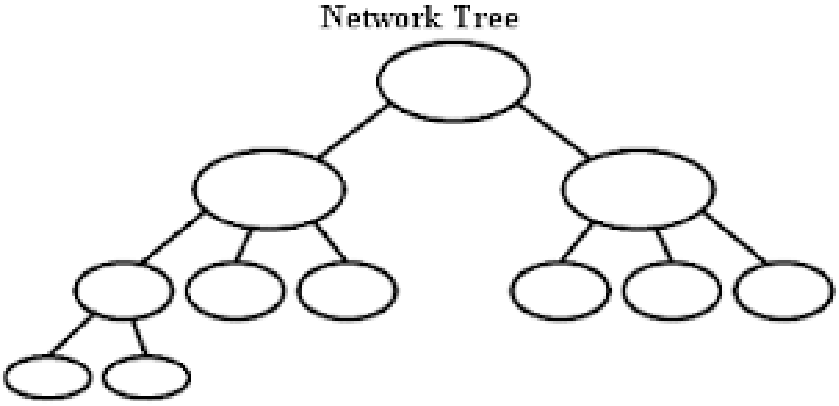


Fig 10.1 Network Topology Structure

Full Mesh Network

- Each OSPF (Open Shortest Path First) router sends topology information to each adjacent neighbor within an area (flooding domain). If Router A receives a new link-state advertisement (LSA), Router D receives three copies of this new LSA: one from Router A, one from Router B, and one from Router C. The Cisco IOS Software implementation of OSPF does have an option to control the flooding through a full mesh network, using the database filter-out command.
- IS-IS is similar to OSPF; each router sends topology information to each adjacent neighbor. Cisco IOS Software enables you to control flooding through mesh groups.
- Each router in an EIGRP (Enhanced Interior Gateway Routing Protocol) network

sends each of the routes it is using to forward traffic to each neighbor. In this network, Router D is going to receive three copies of any new routing information that Router A receives, one copy from Router A, one from Router B, and one from Router C. These three copies of the routing information might be the same, but they indicate reachability through three different next hops (or neighbors). Reducing the information propagated through the mesh is difficult, at best. You can filter these routing updates through some paths within the mesh to decrease the amount of information flooded through the mesh, but that also reduces the number of paths usable through the mesh for any specific destination.

OSPF and IS-IS flood extra information through a mesh topology by default, but you can use tools to reduce the amount of flooding in highly meshed topologies. EIGRP sends updates through each router in the mesh, but it is difficult to reduce the number of these updates unless you want to decrease the number of paths that the network actually uses through the mesh.

In the real world, OSPF and IS-IS scale better in highly meshed environments, especially if you implement flooding reduction techniques. This is a matter of scale, of course; networks that have a mesh network of 20 or 30 routers work fine with any of the three routing protocols. However, when the mesh starts surpassing this number of routers, the special techniques that OSPF and IS-IS offer to scale further can make a difference.

Interaction with Hierarchical Designs

- Traditional network design is based on layers, either two or three, that abstract the network details into ”black boxes” and divide functionality vertically through the network to make management and design easier:
- The two-layer model has aggregation and core layers, or areas, within the network.
- The three-layer model has access, distribution, and core layers.
-
- OSPF splits flooding domains into areas that are separated by ABRs. Because every router within an area must share the same link-state database to calculate

- loop-free paths through the network, the only place that route aggregation can be performed is at an ABR. ABRs actually aggregate two types of information:
- Information about the topology of an area that is hidden from other areas at these border edges.
- Aggregation of reachability information that can be configured at these border edges.

This combination of route aggregation points and flooding domain boundaries in the network implies several things:

- In all three-layer network designs with OSPF, you should place the ABR in the distribution layer of the network.
- In all two-layer network designs with OSPF, you should place the ABR at the aggregation to the core layer edge of the network.
- The most aggregation points that you can cross when passing from one edge of the network to the opposite edge of the network is two.

These topological limitations might not be major in smaller networks, but in networks that have thousands of routers, they could impose severe restrictions on the network design. Network designers and operators normally break up OSPF networks at this size into multiple administrative domains, connecting the separate domains through BGP or some other mechanism.

IS-IS is similar to OSPF in its restrictions, except that IS-IS allows the core and outlying flooding domains to overlap. This introduces a degree of flexibility that OSPF does not provide, but you can still only aggregate routing information at the edges where two flooding domains meet, and you cannot build more than two levels of routing into the network.

EIGRP, as a distance vector protocol, does not divide the concepts of topology summarization and routing aggregation; topology beyond one hop away is hidden by the natural operation of the protocol. Figure G-4 illustrates the conceptual difference among EIGRP, OSPF/IS-IS, and RIP in terms of topology information propagated through the network.

Topological Awareness in Routing Protocols

If you examine the scope through which routing information is transmitted (or known) within a network, you find the following:

- The Bellman-Ford algorithm, used by the Routing Information Protocol (RIP) and the Interior Gateway Routing Protocol (IGRP), uses only information about the local cost to reach a given destination. If Router B is running RIP, it considers only the total cost of the path to reach a destination at Router E when deciding on the best (loop-free) path.
- Diffusing Update Algorithm (DUAL), used by EIGRP, considers the local cost to reach a given destination and the cost of each neighbor to reach the same destination when calculating which available paths are loop free. EIGRP uses an awareness of the topology that is one hop away from the calculating router.
- OSPF and IS-IS, which are link-state protocols, do not use information about the metrics of a neighbor; rather, they count on being aware of the entire topology when calculating a loop-free path. At a flooding domain border, OSPF and IS-IS act much like distance vector protocols. Router A does not know about the topology behind Router B; it only knows the cost of Router B to reach destinations that are attached to Router E.

Because topology information is hidden in the natural processing of EIGRP routing updates, EIGRP is not restricted in where it can aggregate routing information within the network. This provides a great deal of flexibility to network designers who are running EIGRP. Multiple layers of aggregation can be configured in the network. This means that moving from one edge of the network to the opposite edge of the network could mean encountering many more than two aggregation points.

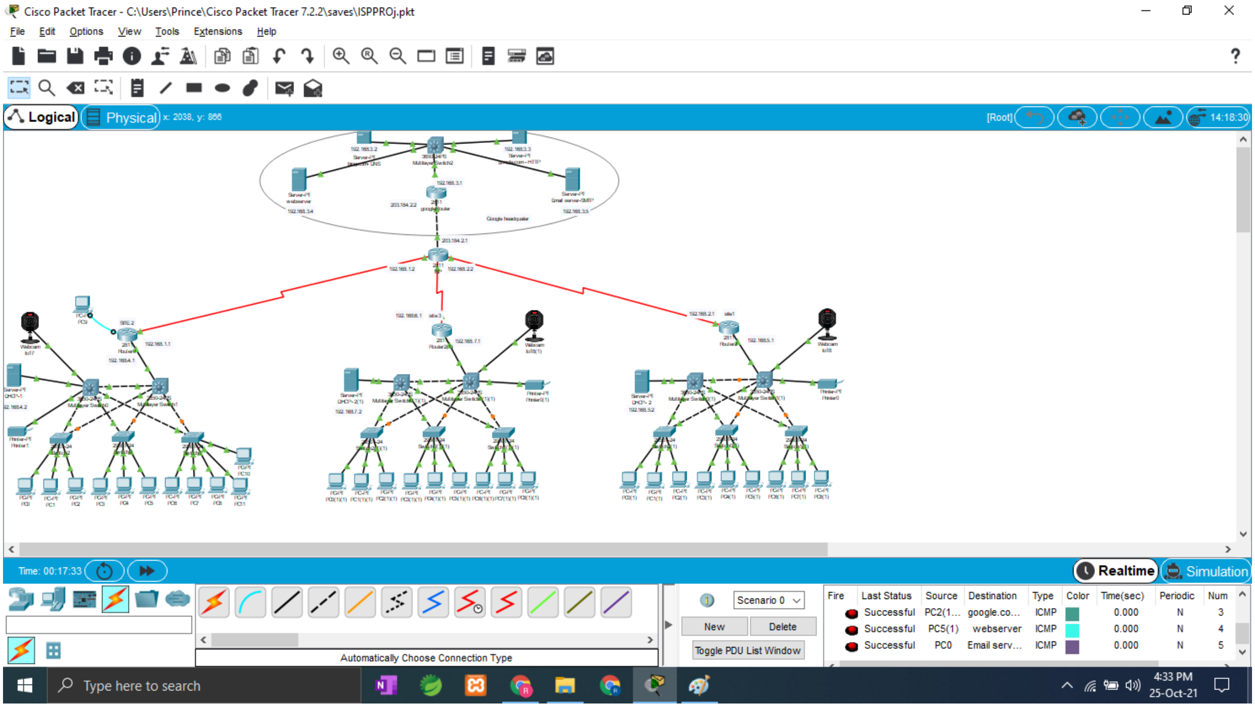
The practical result of the EIGRP capability to aggregate routing information anywhere in the network is that many existing large-scale (2000 router and larger) networks run within a single EIGRP process or administrative domain. The feasibility of building networks this large is based on the capability to use route aggregation to divide the network into multiple layers, or sections, each acting fairly independently of the other. Although it is possible to build an OSPF or IS-IS network this large, designing and managing this network is more difficult because of the restrictions that link-state protocols place on aggregation points.

In general, up to some relative size, the protocols are relatively equal in their capability to work with hierarchical network designs. OSPF and IS-IS tend to be less flexible about where route aggregation can be placed in the network, making it more difficult, in some situations, to fit the network design and the protocol design together. EIGRP excels at fitting into hierarchical network design.

11. Network Design (Topology Created)

- The Internet Cafe consists of 3 branches and a main branch(google headquarters)
- Each branch has a requirement of :
    - 12 PCs
    - Webcams
    - Printers
    - DHCP server
- The Main Branch Office consists of multiple servers.
- Star/Mesh Topology configured in wired networks.
- Network Protocol Applied is IPv4

Simulation of sending packets from Pc to Google server, web server and email server:

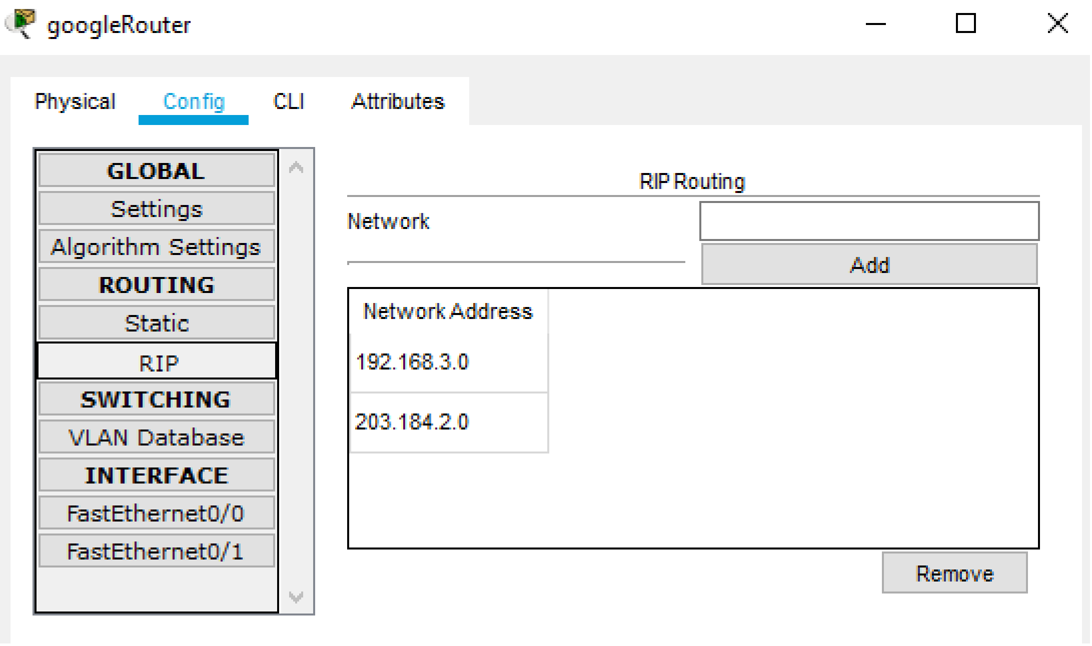


Cisco Packet Tracer - C:\Users\Prince\Cisco Packet Tracer 7.2.2\saves\ISPPROj.pkt

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
●	Successful	PC2(1...	google.co...	ICMP	🟩	0.000	N	3
●	Successful	PC5(1)	webserver	ICMP	🟦	0.000	N	4
●	Successful	PC0	Email serv...	ICMP	🟪	0.000	N	5

Fig. 11.1: Reatime Simulation

RIP table for google router:



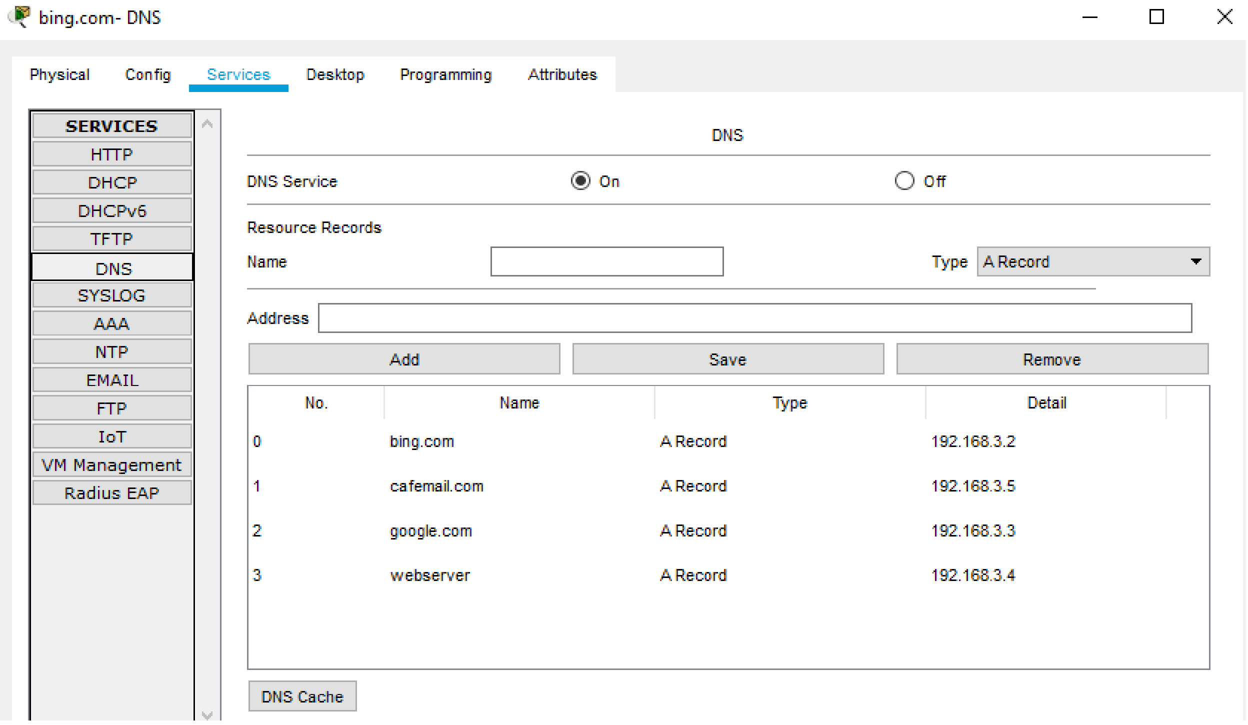
RIP Routing

Network

Network Address
192.168.3.0
203.184.2.0

Fig.11.2: RIP table of google router

DNS Server(containing IP address of all servers):



DNS

DNS Service ● On ○ Off

Resource Records

Name

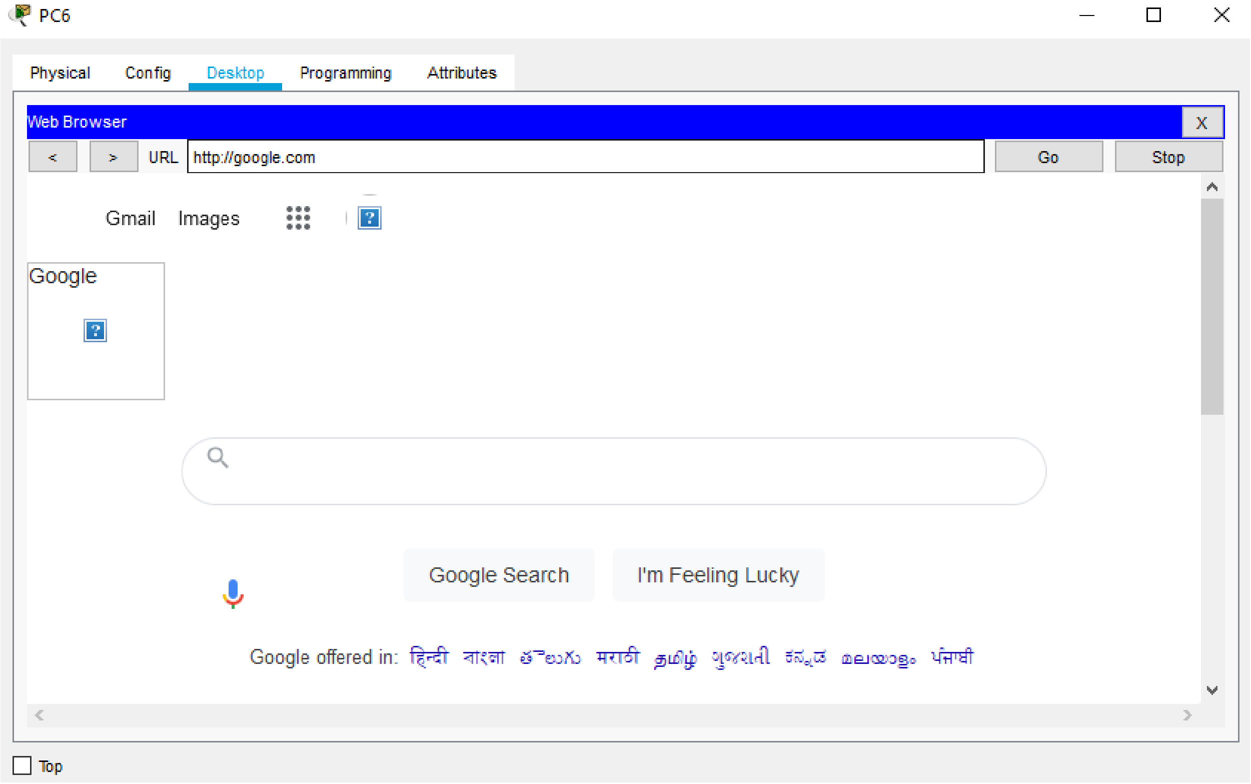
Type A Record

Address

No.	Name	Type	Detail
0	bing.com	A Record	192.168.3.2
1	cafemail.com	A Record	192.168.3.5
2	google.com	A Record	192.168.3.3
3	webserver	A Record	192.168.3.4

Fig.11.3: DNS Server

Accessing google website on any PC in cafe:



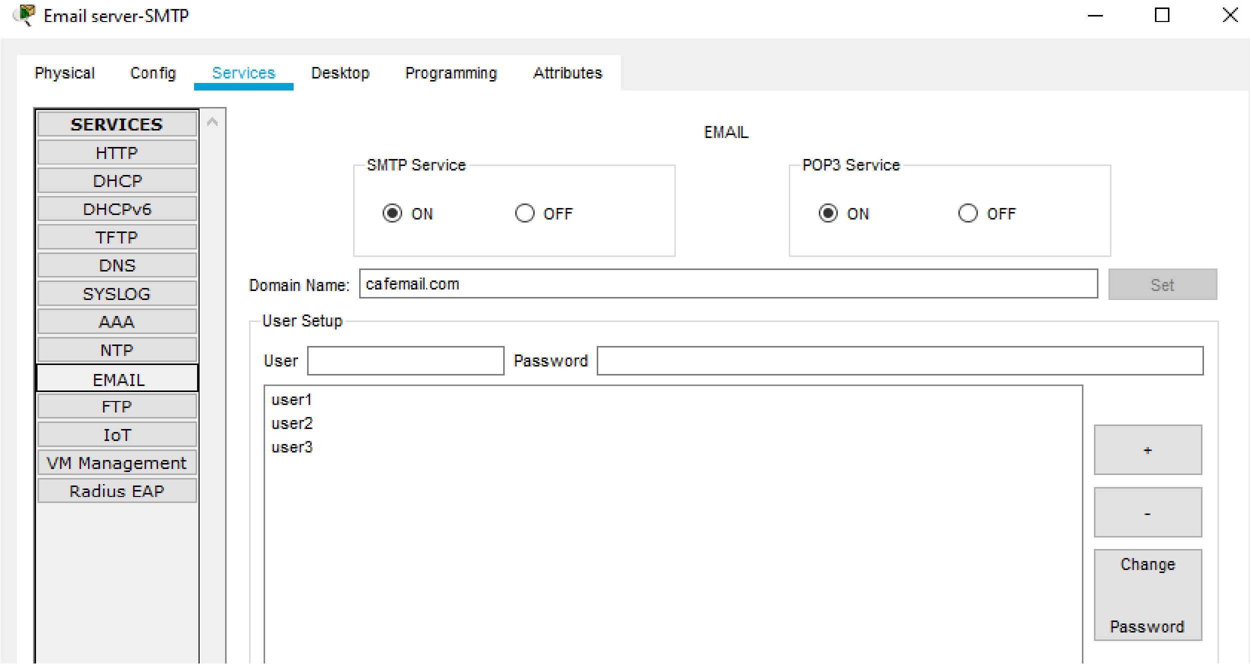
PC6

URL http://google.com

Google offered in: हिन्दी বাংলা తెలుగు मराठी தமிழ் ગુજરાતી ಕನ್ನಡ മലയാളം ਪੰਜਾਬੀ

Fig.11.4: Accessing google website

SMTP server connected to google router also showing no of users :



Email server-SMTP

SMTP Service ● ON ○ OFF

POP3 Service ● ON ○ OFF

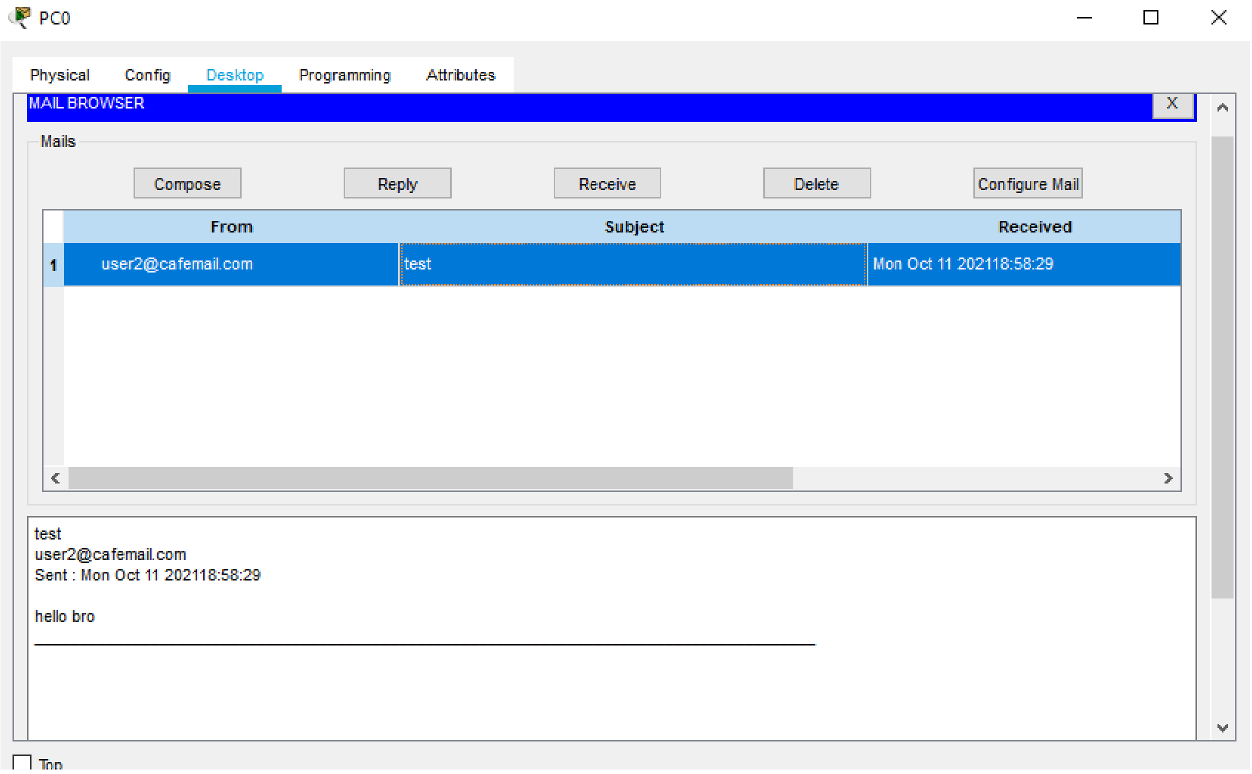
Domain Name: cafemail.com

User   Password

user1
user2
user3

Fig.11.5: SMTP Server

Accessing SMTP server on any Pc in Cafe:



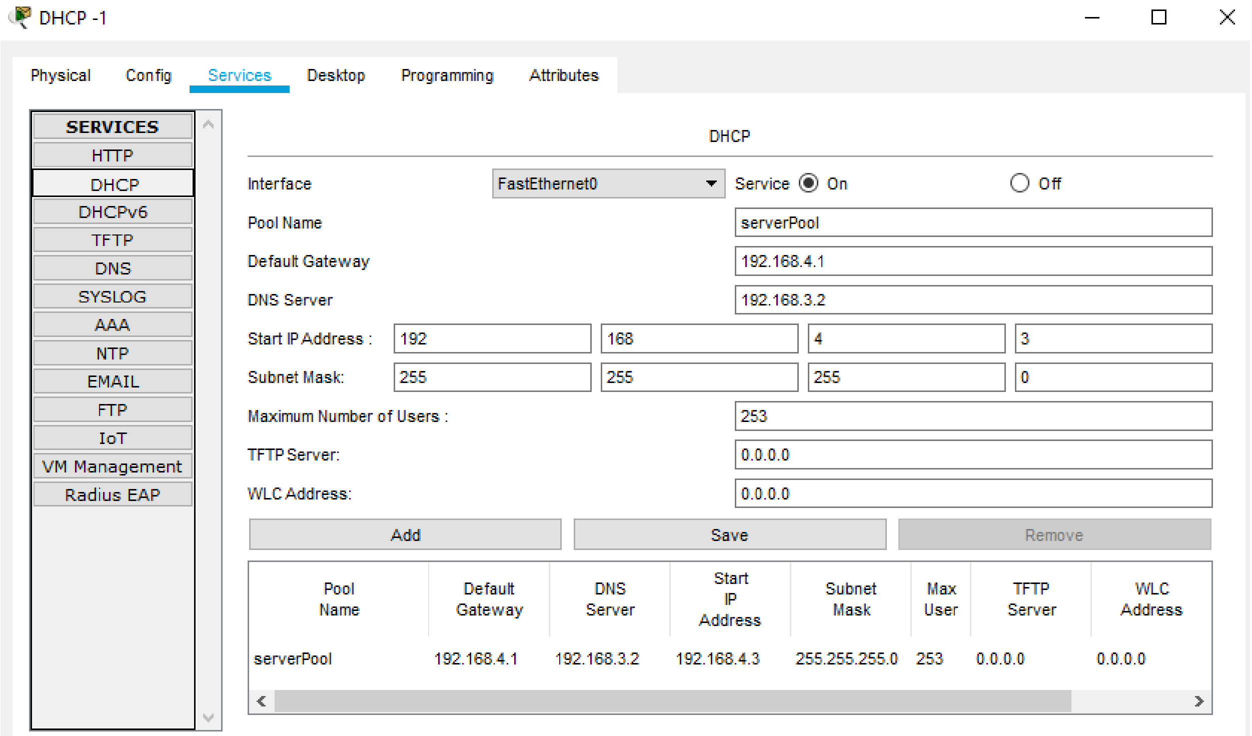
	From	Subject	Received
1	user2@cafemail.com	test	Mon Oct 11 202118:58:29

test
user2@cafemail.com
Sent : Mon Oct 11 202118:58:29

hello bro

Fig.11.6:Accessing SMTP server

DHCP Setting for each branch of cafe:



Interface: FastEthernet0 Service ● On ○ Off

Pool Name: serverPool

Default Gateway: 192.168.4.1

DNS Server: 192.168.3.2

Start IP Address : 192 168 4 3

Subnet Mask: 255 255 255 0

Maximum Number of Users : 253

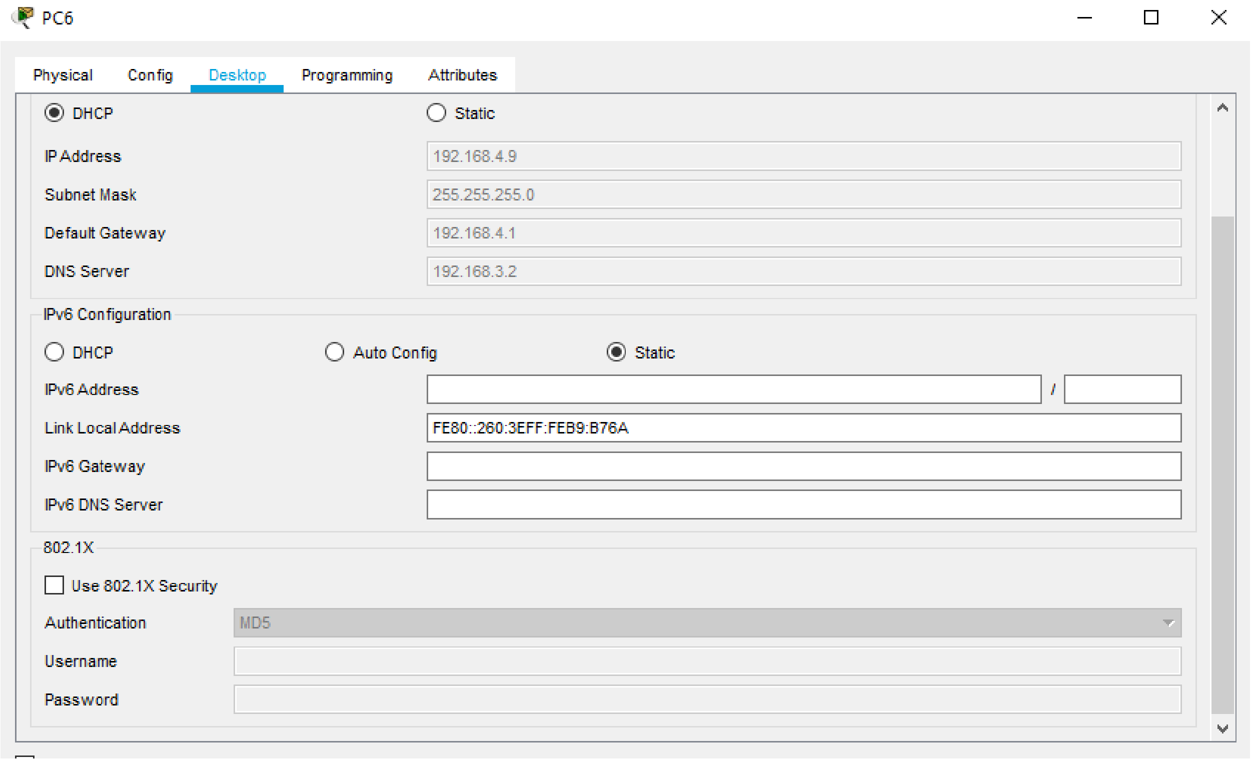
TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.4.1	192.168.3.2	192.168.4.3	255.255.255.0	253	0.0.0.0	0.0.0.0

Fig.11.7: DHCP Server

Successful DHCP connection for any Pc in each branch of Cafe:



PC6

● DHCP ○ Static

IP Address	192.168.4.9
Subnet Mask	255.255.255.0
Default Gateway	192.168.4.1
DNS Server	192.168.3.2

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address	/
Link Local Address	FE80::260:3EFF:FEB9:B76A
IPv6 Gateway	
IPv6 DNS Server	

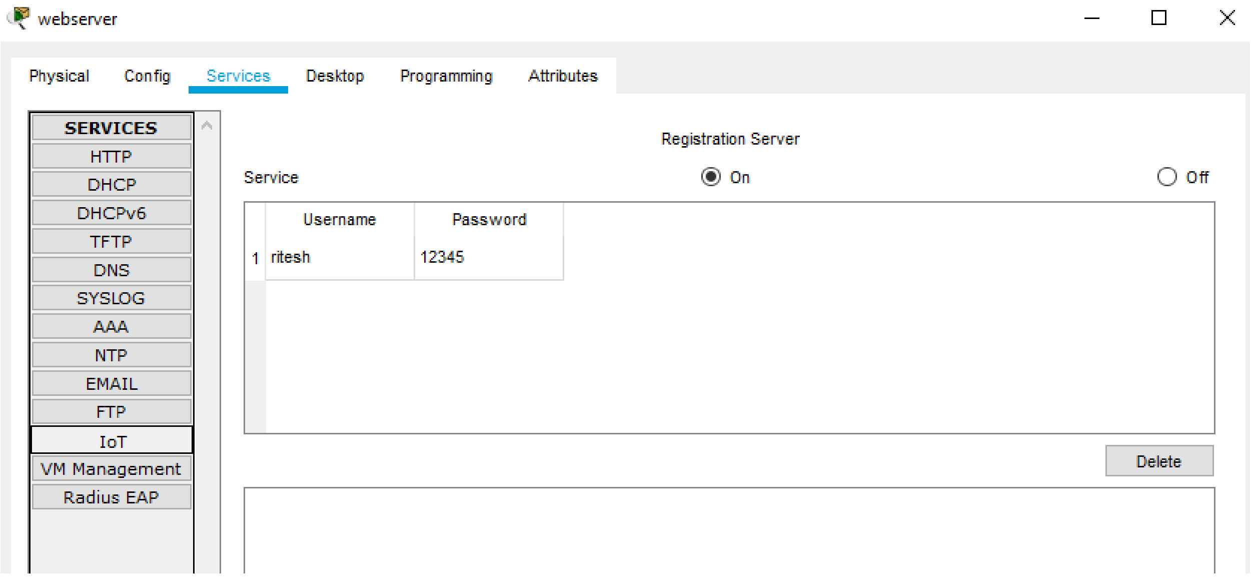
802.1X

□ Use 802.1X Security

Authentication	MD5
Username	
Password	

Fig.11.8: DHCP Connection at PC

IOT Server Setting with one admin user:



webserver

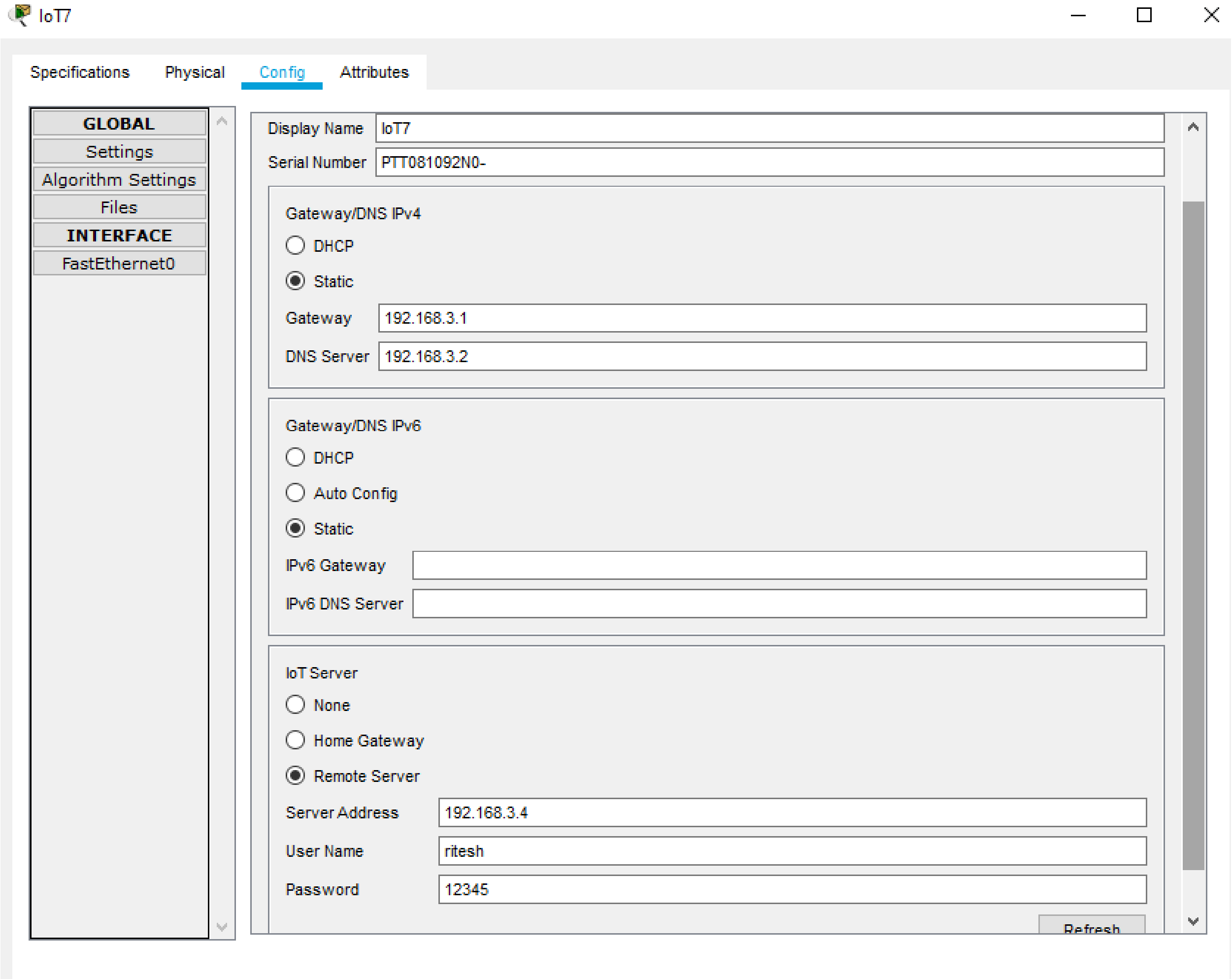
Registration Server

Service ● On ○ Off

	Username	Password
1	ritesh	12345

Fig.11.9: IOT Server

IOT device setting for connecting it to server:



Display Name: IoT7

Serial Number: PTT081092N0-

Gateway/DNS IPv4

○ DHCP

● Static

Gateway: 192.168.3.1

DNS Server: 192.168.3.2

Gateway/DNS IPv6

○ DHCP

○ Auto Config

● Static

IPv6 Gateway:

IPv6 DNS Server:

IoT Server

○ None

○ Home Gateway

● Remote Server

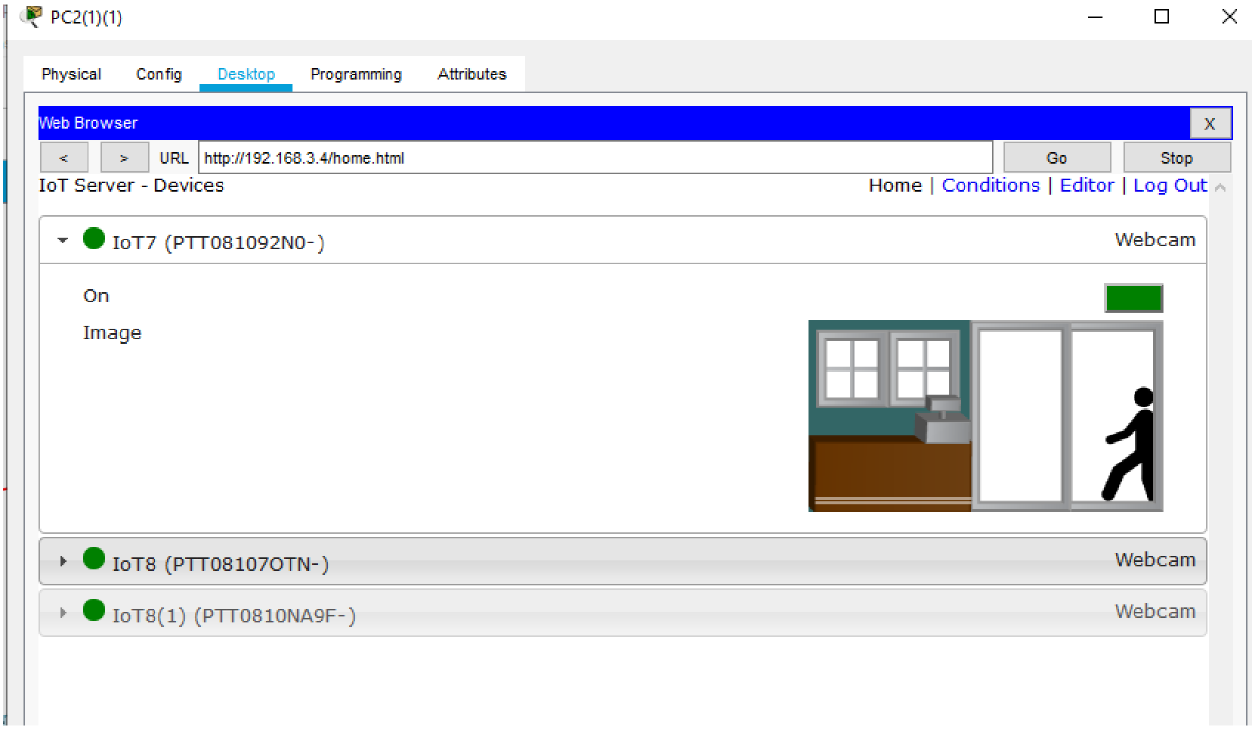
Server Address: 192.168.3.4

User Name: ritesh

Password: 12345

Fig.11.10:IOT Device connection to server

Accessing IOT Server on any PC after login by admin:



http://192.168.3.4/home.html

IoT Server - Devices

Home | Conditions | Editor | Log Out

● IoT7 (PTT081092N0-) Webcam

On

Image

● IoT8 (PTT08107OTN-) Webcam

● IoT8(1) (PTT0810NA9F-) Webcam

Fig.11.11: Accessing IOT server

12. Conclusion

The outcome of the proposed system will be a fail-safe backbone network infrastructure which meets the requirements for readily available access to information and security of the private network, and also ensures optimized productivity when telecommunication services are accessed. It is a reliable and secure network. It can easily give access to all computers equally. There is less risk of virus spreading over the network as secure switches. Computers have been used with moderate specifications which are compatible to run over the network properly.

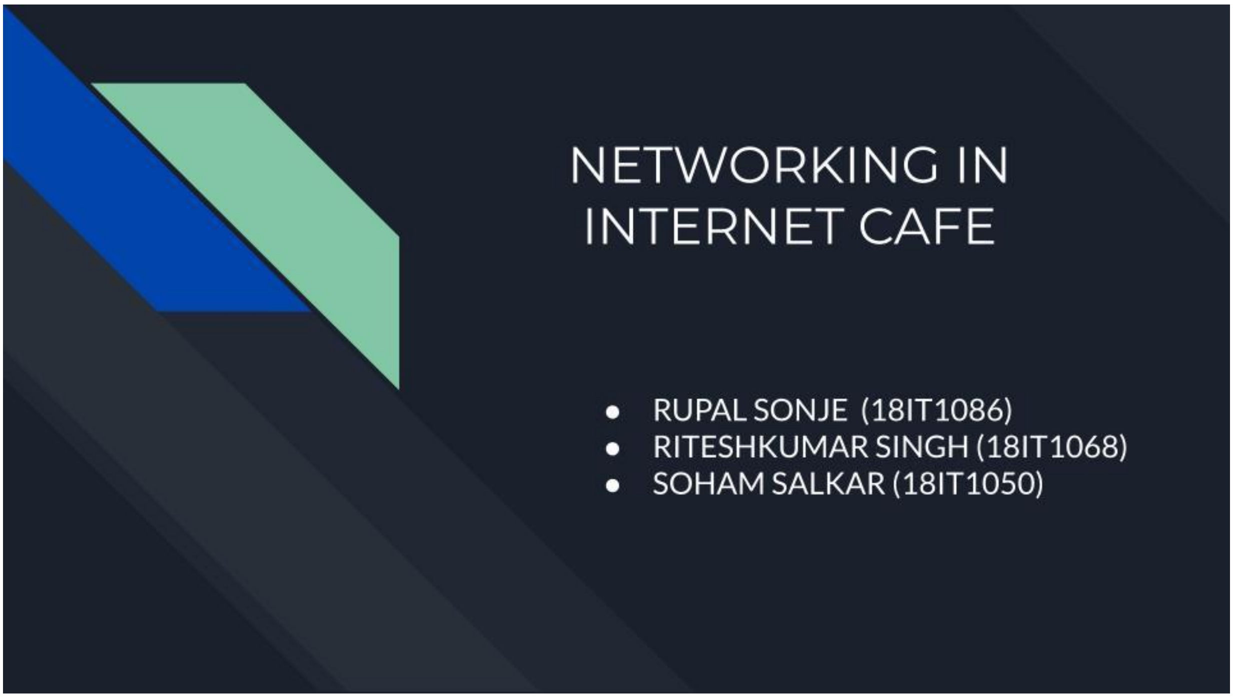
13. References

[1] Yanhong Wang, Hanshi Wang, Lizhen Liu, Wei Song Research and Implementation of Network Planning and Design for Community

[2] Wikipedia. ”Stackable switch”. Internet: https://en.wikipedia.org/wiki/Stackable switch.

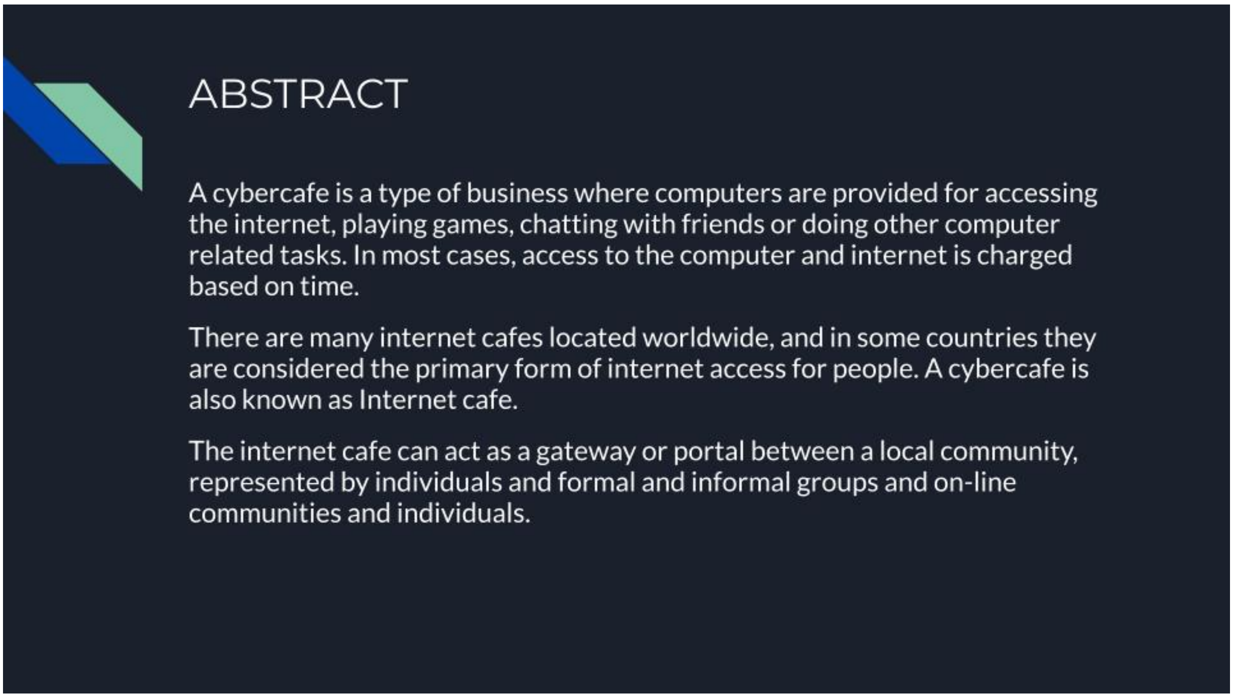
[3] Wikipedia of network planning -https://en.wikipedia.org/wiki/Network planning and design

[4] Wikipedia for Routing Protocol - https://en.wikipedia.org wiki Routing protocol.3



NETWORKING IN INTERNET CAFE

- RUPAL SONJE (18IT1086)
- RITESHKUMAR SINGH (18IT1068)
- SOHAM SALKAR (18IT1050)

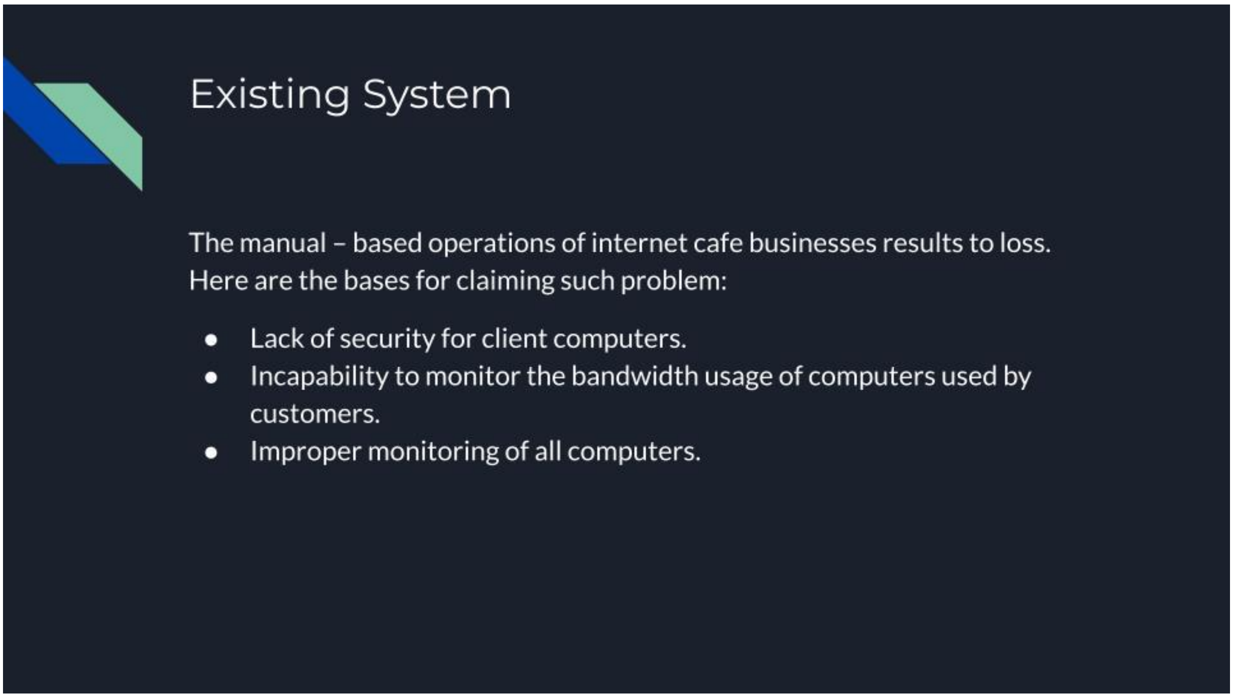


ABSTRACT

A cybercafe is a type of business where computers are provided for accessing the internet, playing games, chatting with friends or doing other computer related tasks. In most cases, access to the computer and internet is charged based on time.

There are many internet cafes located worldwide, and in some countries they are considered the primary form of internet access for people. A cybercafe is also known as Internet cafe.

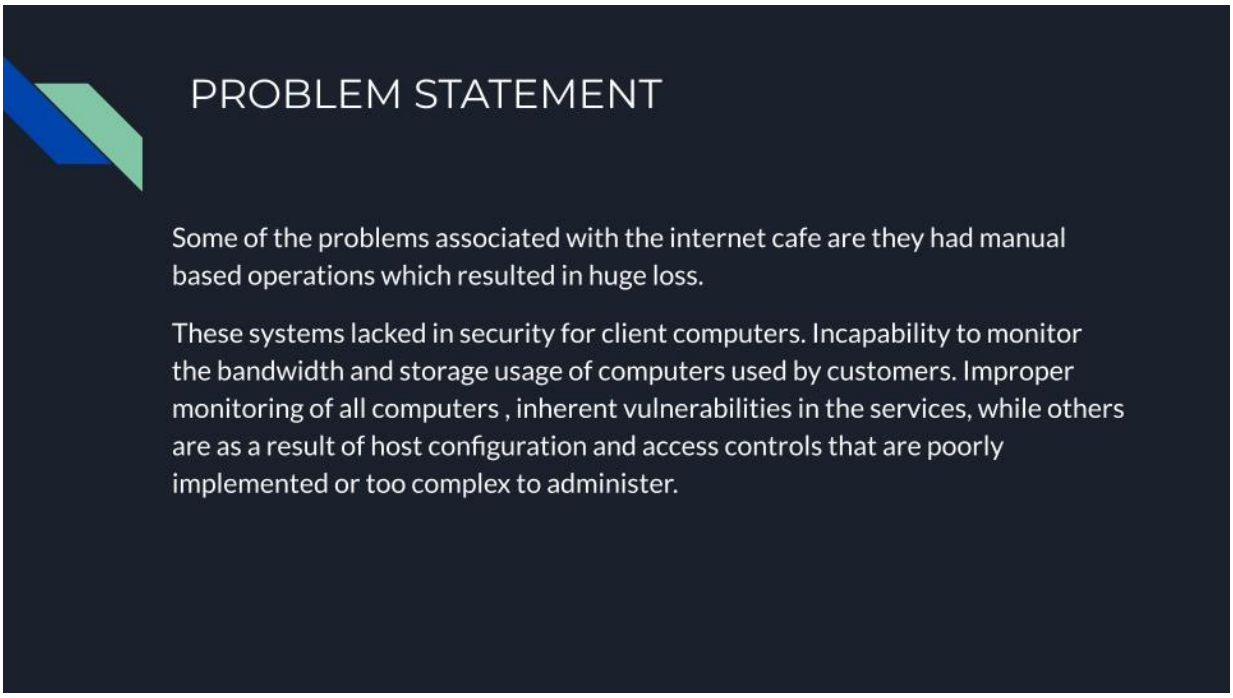
The internet cafe can act as a gateway or portal between a local community, represented by individuals and formal and informal groups and on-line communities and individuals.



Existing System

The manual – based operations of internet cafe businesses results to loss. Here are the bases for claiming such problem:

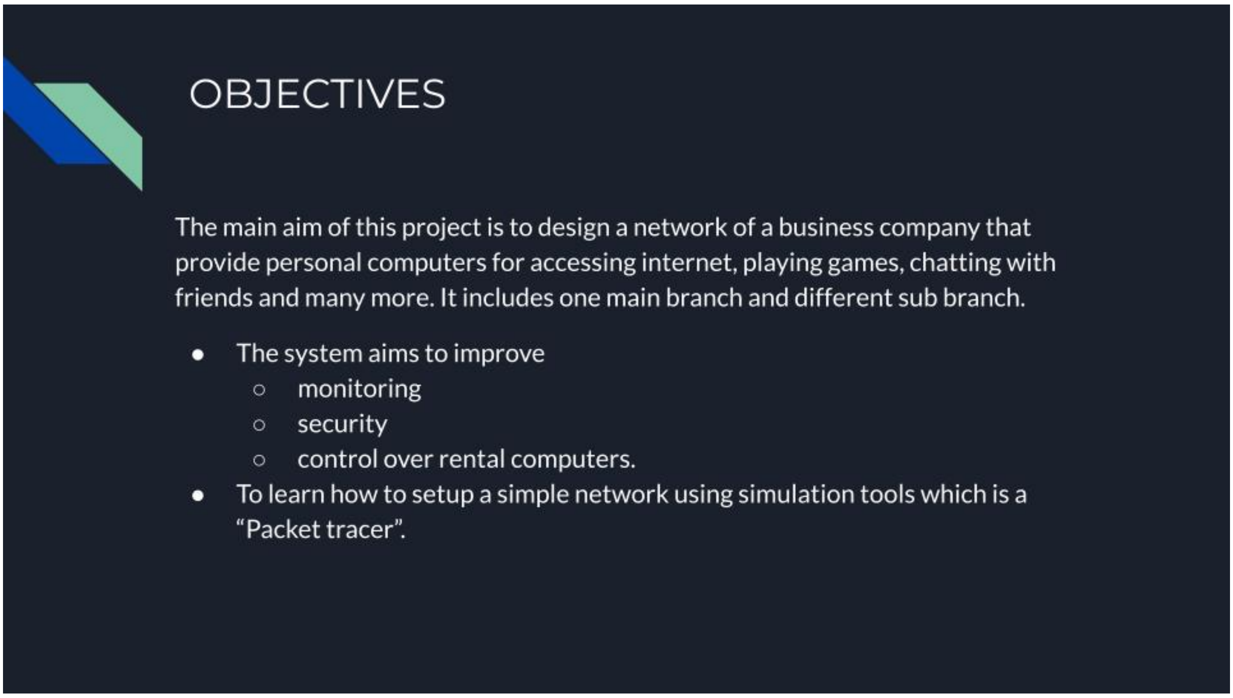
- Lack of security for client computers.
- Incapability to monitor the bandwidth usage of computers used by customers.
- Improper monitoring of all computers.



PROBLEM STATEMENT

Some of the problems associated with the internet cafe are they had manual based operations which resulted in huge loss.

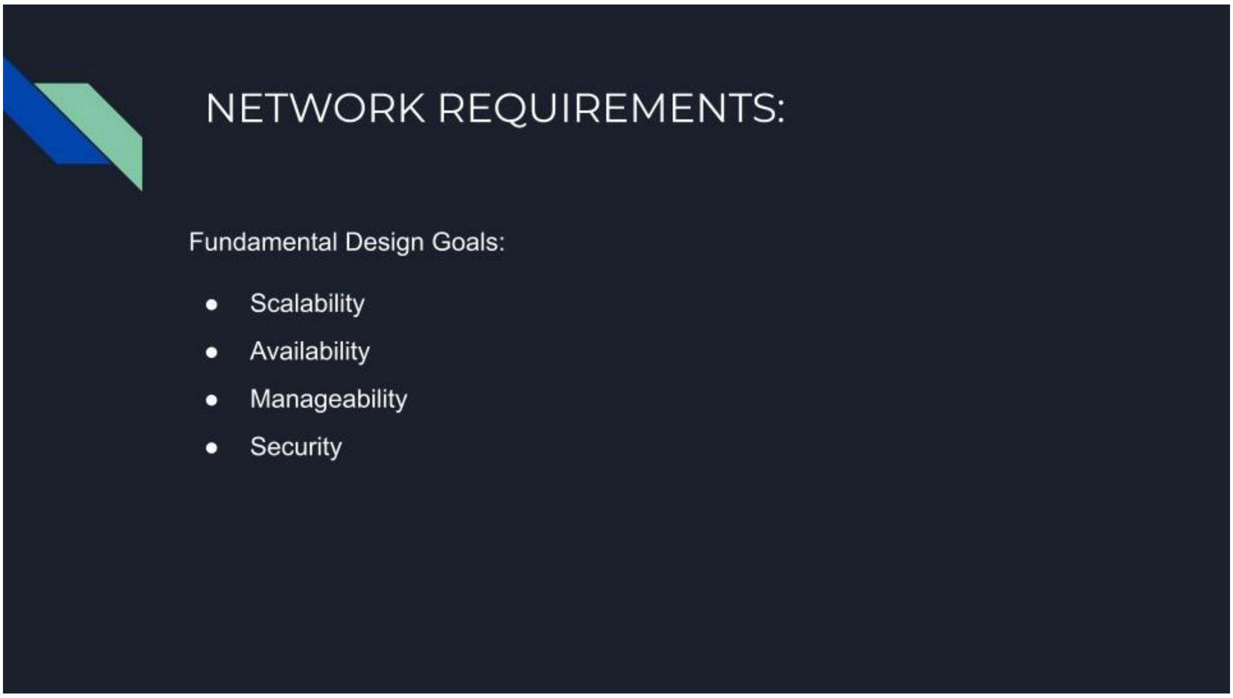
These systems lacked in security for client computers. Incapability to monitor the bandwidth and storage usage of computers used by customers. Improper monitoring of all computers , inherent vulnerabilities in the services, while others are as a result of host configuration and access controls that are poorly implemented or too complex to administer.



OBJECTIVES

The main aim of this project is to design a network of a business company that provide personal computers for accessing internet, playing games, chatting with friends and many more. It includes one main branch and different sub branch.

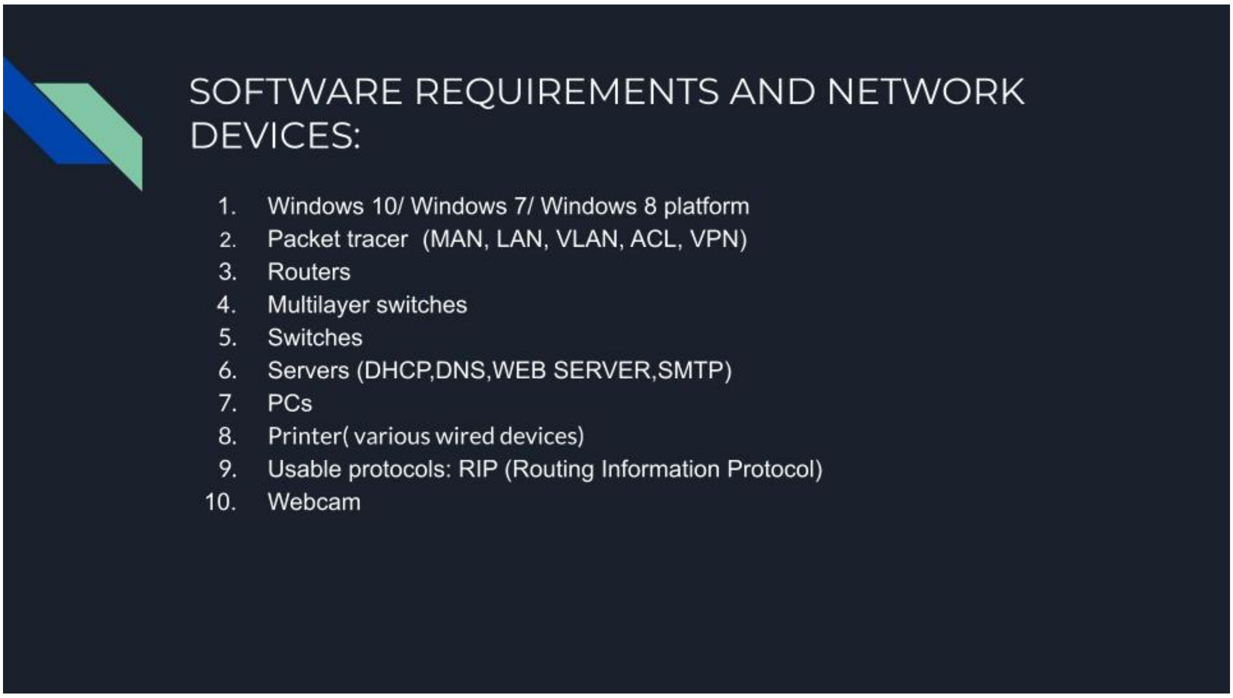
- The system aims to improve
  - monitoring
  - security
  - control over rental computers.
- To learn how to setup a simple network using simulation tools which is a "Packet tracer".



NETWORK REQUIREMENTS:

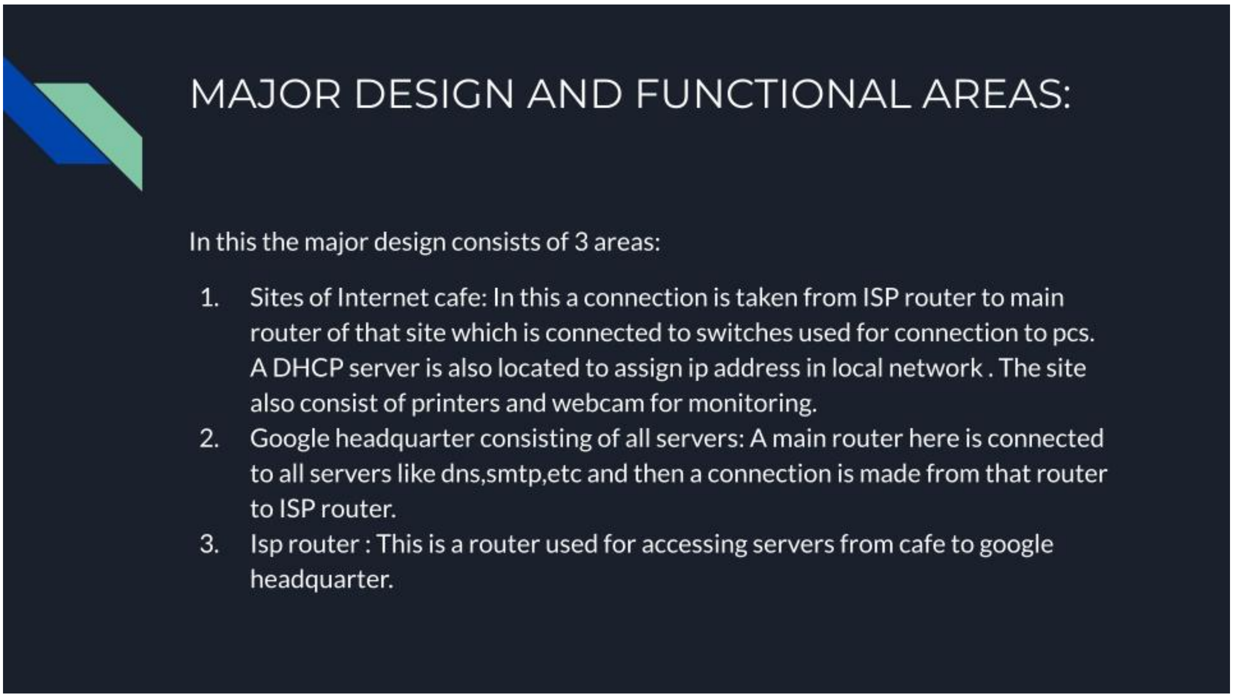
Fundamental Design Goals:

- Scalability
- Availability
- Manageability
- Security



SOFTWARE REQUIREMENTS AND NETWORK DEVICES:

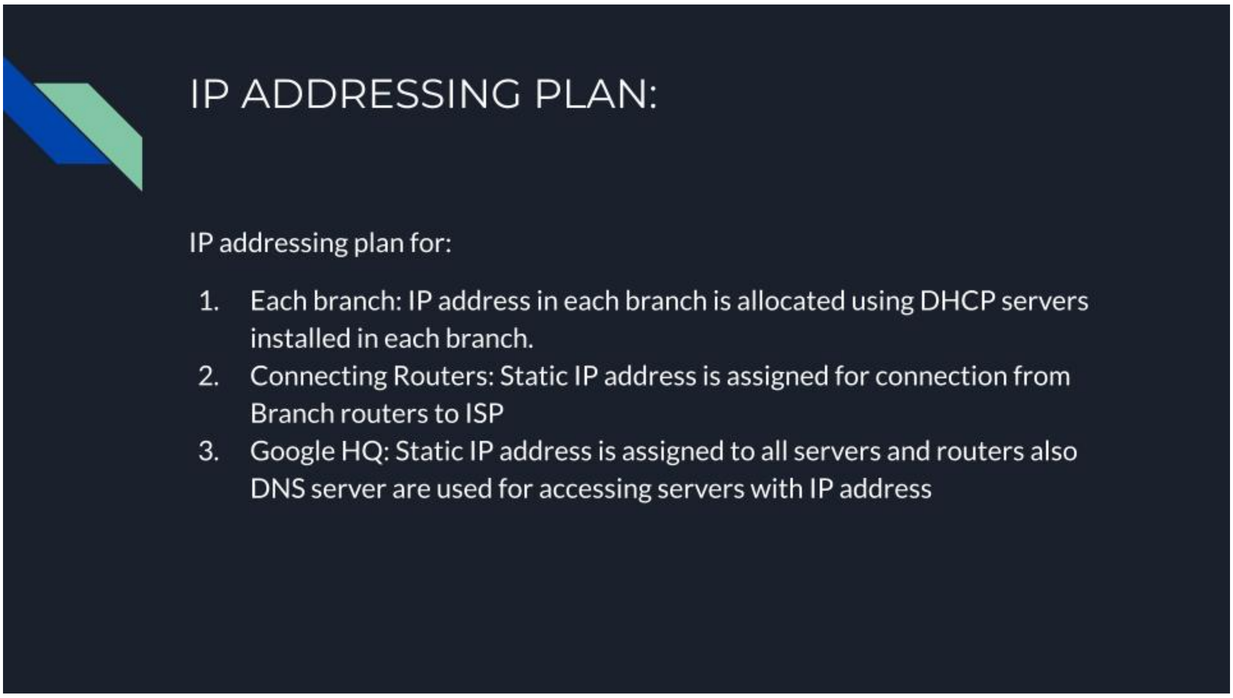
1. Windows 10/ Windows 7/ Windows 8 platform
2. Packet tracer (MAN, LAN, VLAN, ACL, VPN)
3. Routers
4. Multilayer switches
5. Switches
6. Servers (DHCP,DNS,WEB SERVER,SMTP)
7. PCs
8. Printer(various wired devices)
9. Usable protocols: RIP (Routing Information Protocol)
10. Webcam



MAJOR DESIGN AND FUNCTIONAL AREAS:

In this the major design consists of 3 areas:

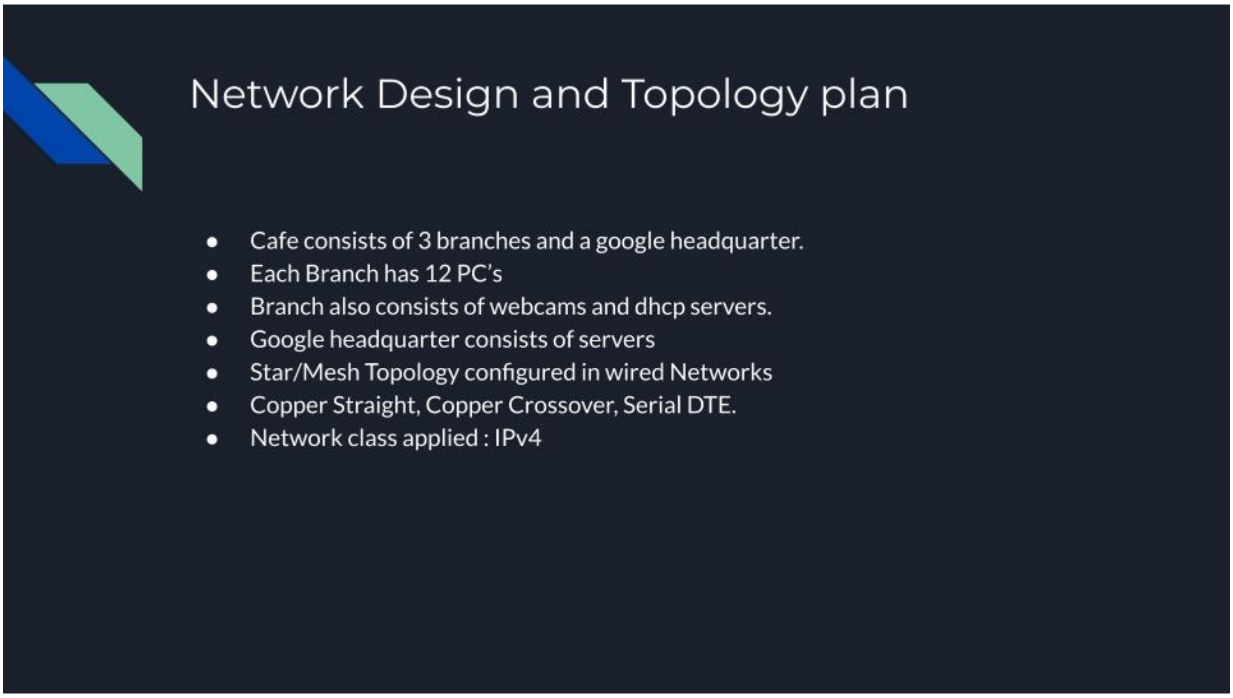
1. Sites of Internet cafe: In this a connection is taken from ISP router to main router of that site which is connected to switches used for connection to pcs. A DHCP server is also located to assign ip address in local network . The site also consist of printers and webcam for monitoring.
2. Google headquarter consisting of all servers: A main router here is connected to all servers like dns,smtp,etc and then a connection is made from that router to ISP router.
3. Isp router : This is a router used for accessing servers from cafe to google headquarter.



IP ADDRESSING PLAN:

IP addressing plan for:

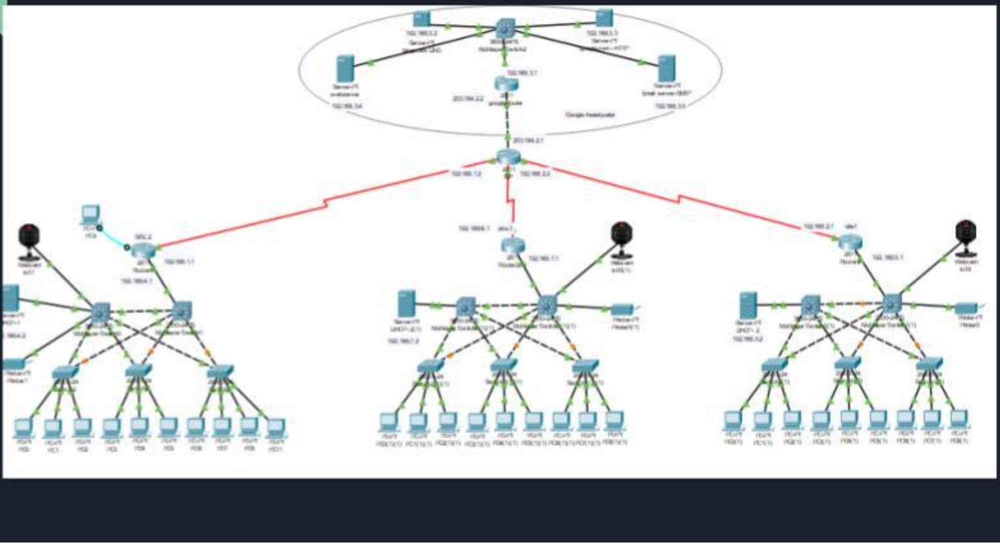
1. Each branch: IP address in each branch is allocated using DHCP servers installed in each branch.
2. Connecting Routers: Static IP address is assigned for connection from Branch routers to ISP
3. Google HQ: Static IP address is assigned to all servers and routers also DNS server are used for accessing servers with IP address



Network Design and Topology plan

- Cafe consists of 3 branches and a google headquarter.
- Each Branch has 12 PC's
- Branch also consists of webcams and dhcp servers.
- Google headquarter consists of servers
- Star/Mesh Topology configured in wired Networks
- Copper Straight, Copper Crossover, Serial DTE.
- Network class applied : IPv4

Design:



CONCLUSION

This has been concluded from this project that it is reliable and secure network. It can easily give access to all the computers equally. There is less risk of virus spreading over the network as secure switches have been used which gives the high profile for Firewall and other activities. Computers have been used with moderate specifications which are compatible to run over network properly.