ENTERPRISE NETWORK DESIGN
NATIONAL BANK NATIONAL NETWORK

University of New Haven
Tagliatela College of Engineering

Enterprise Network Design Project
Submitted by
Group – 2
CSCI – 6649 – 01 : Enterprise Network Design

Professor. Syed Hussein

Project Team
Sowmya Kala (Lead)
Kamal Siddharth Teki
Vineetha Unnam
Srihari Chitikela
Vasantha Vemula
Siddhartha
Akhil

May 2022

Abstract

In this project we will primarily focus on design and implementation of National Bank National Network suing Cisco Packet Tracer (CPT). Security breach in the sector of banks is one of the most important concerns that needs to be addressed in the first place since loss of information can lead to huge losses to the bank overall. This project will help us curb such concerns by understanding the regulated flow of information/data. We will consider a national bank which has its head offices located in big cities like New York and Minneapolis. The other small buildings (banks) will be present in major cities like New Haven, East Haven and International sites like Toronto which is located in Canada since good accessibility to customers is mandatory. These small buildings in each state will be connected through LANs. Apart from this, VLANs and WANs will automatically be a part of the project networking since we are working on a National Level Bank Network. Additionally, bank machines will be made available all around each city in specific to ensure better reach and reliable services to the people. Employees use a special software to access user accounts. The level of access to advanced resources within the bank varies from employee to employee based upon several criteria which include the designation of the employee, criticality of the information etc. The typical servers, mail, web, files and directories will be made available to all the employees to understand the flow of work within the bank.

Phase 1

Customer Needs & Goals

Customer Goals & Needs

Chase Bank is a major bank that serves consumers across the United States with a comprehensive range of financial and banking services. Chase Bank administers corporate, commercial, and personal accounts and provides financial services to many consumers. The bank has several locations in major cities and has set up banking services in several small buildings. Thousands of people work in major cities, while hundreds work in tiny towns, according to the bank's many departments. The bank was created as an end-to-end solution to organize the many financial procedures, and employees use a variety of software tools. They want to relocate a huge infrastructure that can accommodate many people while also guaranteeing that their new design is more secure and flexible.

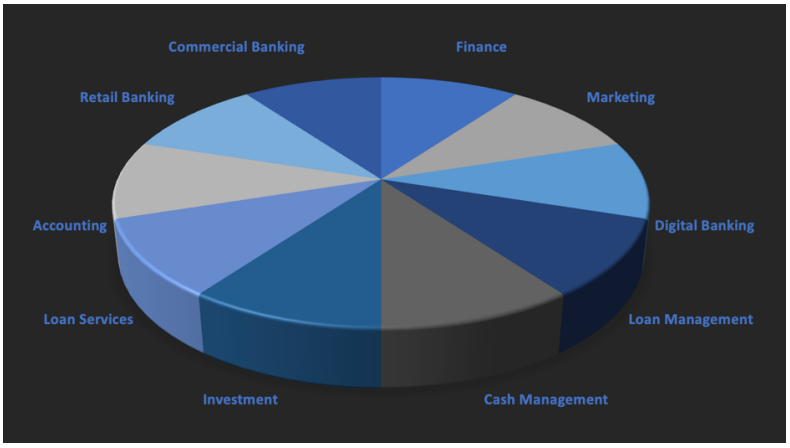
Business Goals

- Secured Banking services
- Operational Excellence
- Safeguarding Integrity and Fairness
- Secured User Transactions & User Data
- Hassle Free Customer Services

Technical Goals

- To provide 24*7 banking services to customers.
- To provide a safe and secured banking environment for the customers.
- To provide multiple banking services for a greater reach across the nation.
- To improve the response time for online transactions & online banking services.

Banking Departments



Network Applications

The applications in this network model are connected via the client-server-cloud network model. These applications are housed on different servers and the server programs builds an active directory to configure the users' access. There are different types of network applications in this design and they are :

- Digital banking
- Commercial Banking
- Retail Banking
- Mortgage Banking
- Cash Management
- Loan Services
- Accounting
- Email Services
- Marketing and Sales

User Communities :

Department	Community Size	Applications Used
Retail Department	110	Cash Management, Retail Banking, Sales, Email Services
Marketing Department	230	Retail Banking, Email Services, Marketing and Sales
Accounting Department	180	Cash Management, Loan Services, Sales and Mortgage Banking
Digital Banking Department	1500	Cash Management, Email Services, Web Application
Financial Department	450	Retail Banking, Cash Management, Web Application and Email Services
Investment Department	1200	Investment
HR Department	80	Email Services

Data Storage & Types of Servers

To deliver secure and reliable services to its clients, this banking network requires a secure datastore model. To ensure secure and dependable transactions, the company employs a range of security protocols. The organization oversees numerous storage operations to ensure a secure data model. For several departments, the organization designs storage models. To manage end-to-end operations, the following various data storages must be considered.

- Web Server
- Database Server
- Email Server
- Backup Server
- DHCP Server Setup
- Payment Gateway Server

Citywise IP Connections

CITY	*IP Address*	*Subnet mask*
New York	192.168.2.0	255.255.255.0
Florida	192.168.1.0	255.255.255.0
Georgia	192.168.5.0	255.255.255.0
New Haven	192.168.4.0	255.255.255.0
Torento	192.168.3.0	255.255.255.0
Mineapolis	192.168.0.0	255.255.255.0

Serial Port City Wise Connections

Serial Port Connection	*IP Address*	*Subnet*
Minneapolis to Florida	192.168.6.0	255.255.255.0
Minneapolis to New york	192.168.7.0	255.255.255.0
Minneapolis to New haven	192. 168.14.0	255.255.255.0
Minneapolis to Georgia	192. 168.13.0	255.255.255.0
Minneapolis to Toronto	192. 168.15.0	255.255.255.0
Newyork to Florida	192. 168.17.0	255.255.255.0
New york to Toronto	192. 168.19.0	255.255.255.0
New york to Georgia	192. 168.20.0	255.255.255.0
New york to New haven	192. 168.9.0	255.255.255.0

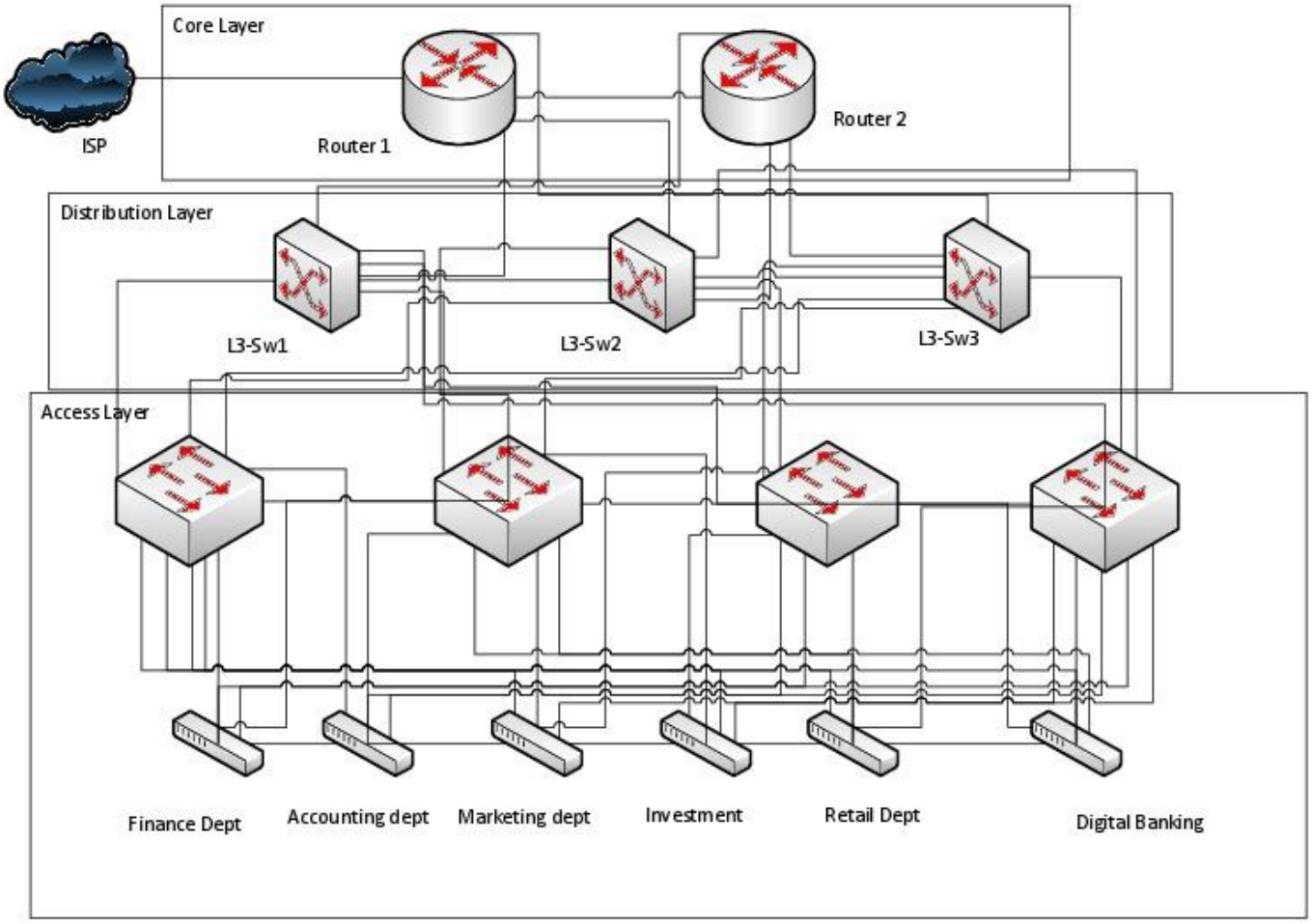
Serial Port City Wise Connections (Continuation)

New haven to Florida	192.168.16.0	255.255.255.0
New haven to Georgia	192.168.11.0	255.255.255.0
New haven to Toronto	192.168.18.0	255.255.255.0
Georgia to Florida	192.168.15.0	255.255.255.0
Georgia to Toronto	192.168.10.0	255.255.255.0
Florida to Toronto	192.168.8.0	255.255.255.0

Phase 2

Logical Design

Network Topology



Access Layer

In this layer, all the end devices are connected to each other to the network and we will be having the layer 1 switch for the further connections.

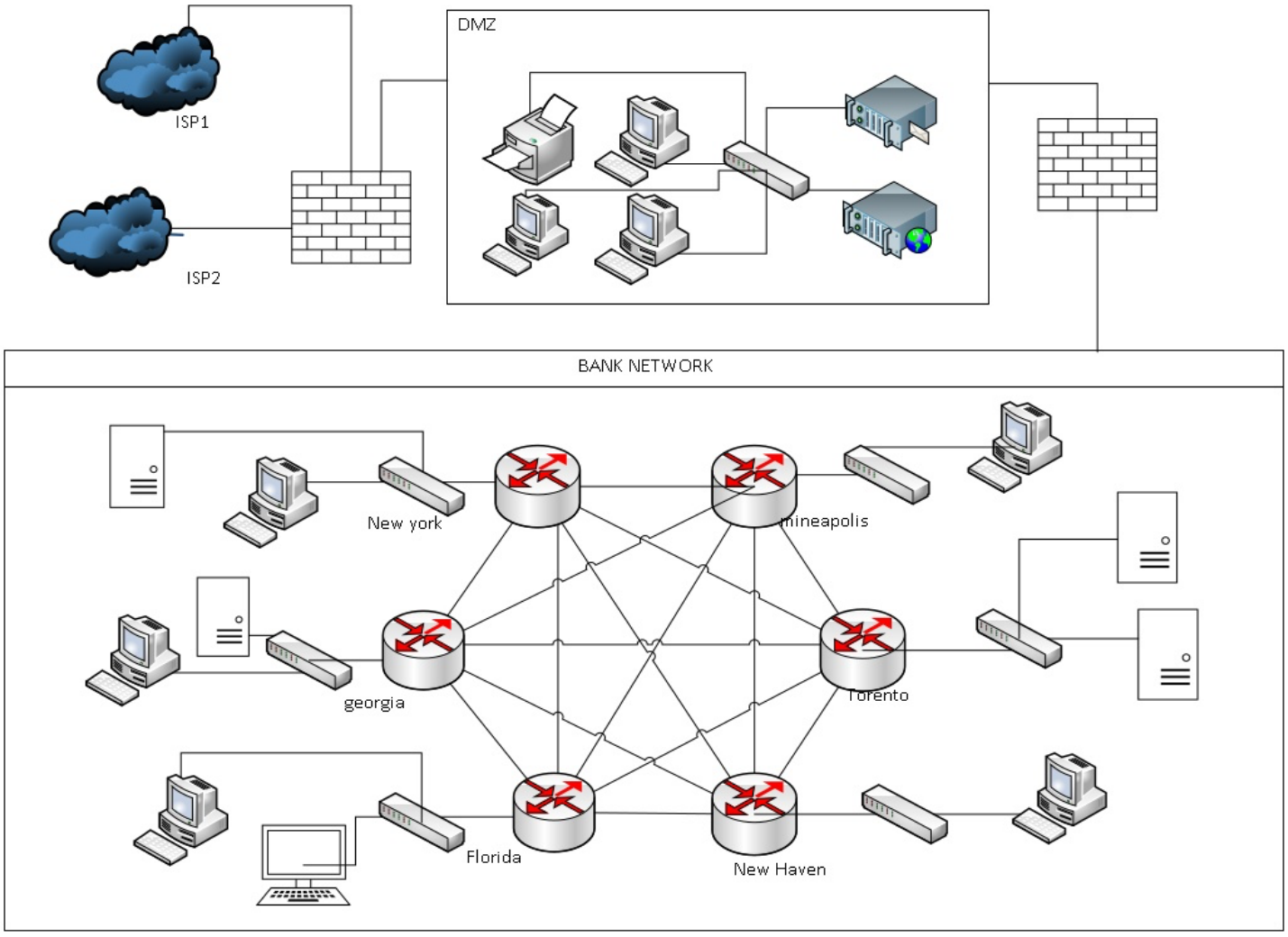
Distribution Layer

In the Distribution layer, mostly the layer 3 switches are used to connect the end devices and make the network correspond and this connects to the access and core layers of the network design.

Core Layer

The core layer is the main source of all the layers, where this layer is used to transfer the large amount of traffic very quickly.

Network Overlay :



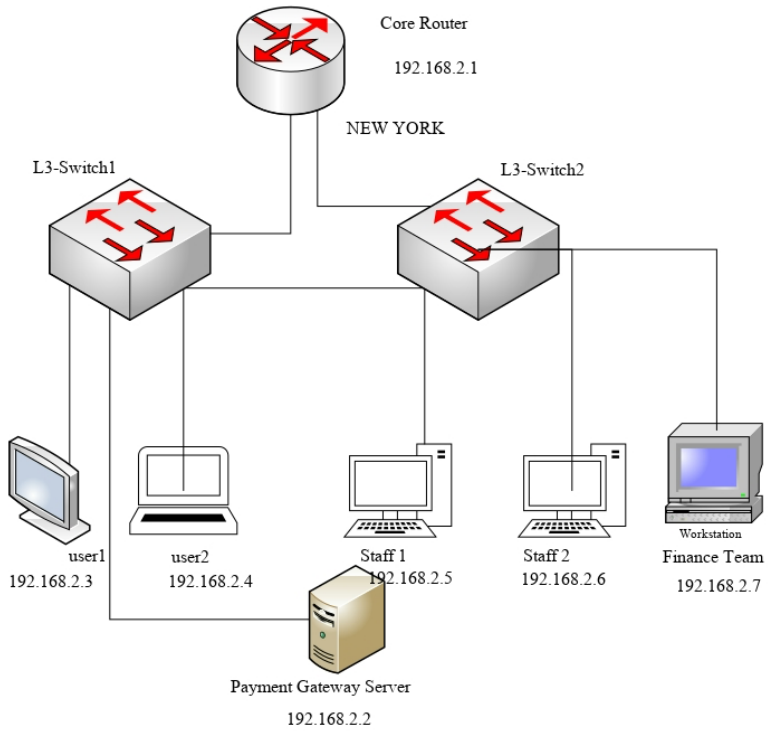
There will be 6 main cities as our branches for this network topology :

- New York
- Georgia
- Florida
- Minneapolis
- New Haven
- Toronto

Each City branch is explained separately for better understanding of the network.

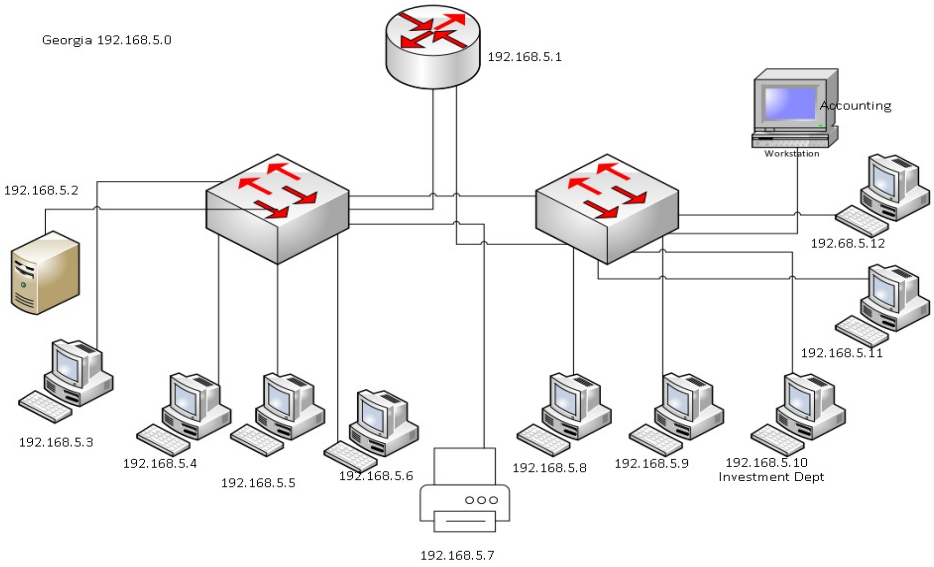
We'll get started with New York network topology and then followed by Georgia, Florida, Minneapolis, New Haven, Toronto network topologies.

New York – Network Topology :



In the New York branch we have 2 campuses which are connected to the core layer router. The IP address for New york city is assigned as 192.168.2.0. The network 192.168.2.1 is assigned as default gateway or router address and 192.168.2.2 is assigned with the server. Rest all the addresses from 192.168.2.3 - 192.168.2.254 are addressed to users and client systems working in the network. Payment gateway server is also configured in this branch for the whole network. Payment gateway server is typically a gateway between merchant bank and customer for online banking.

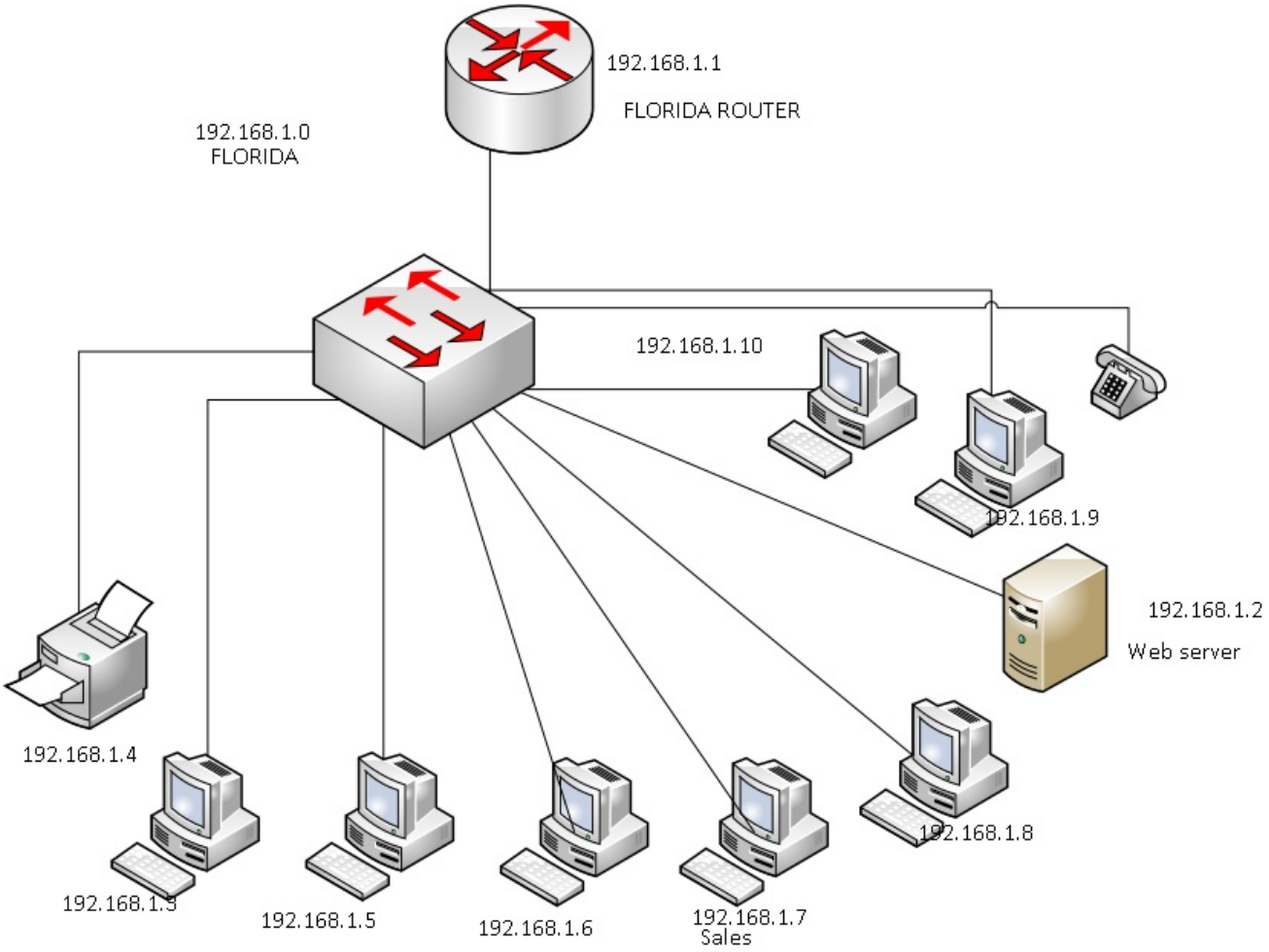
Georgia – Network Topology



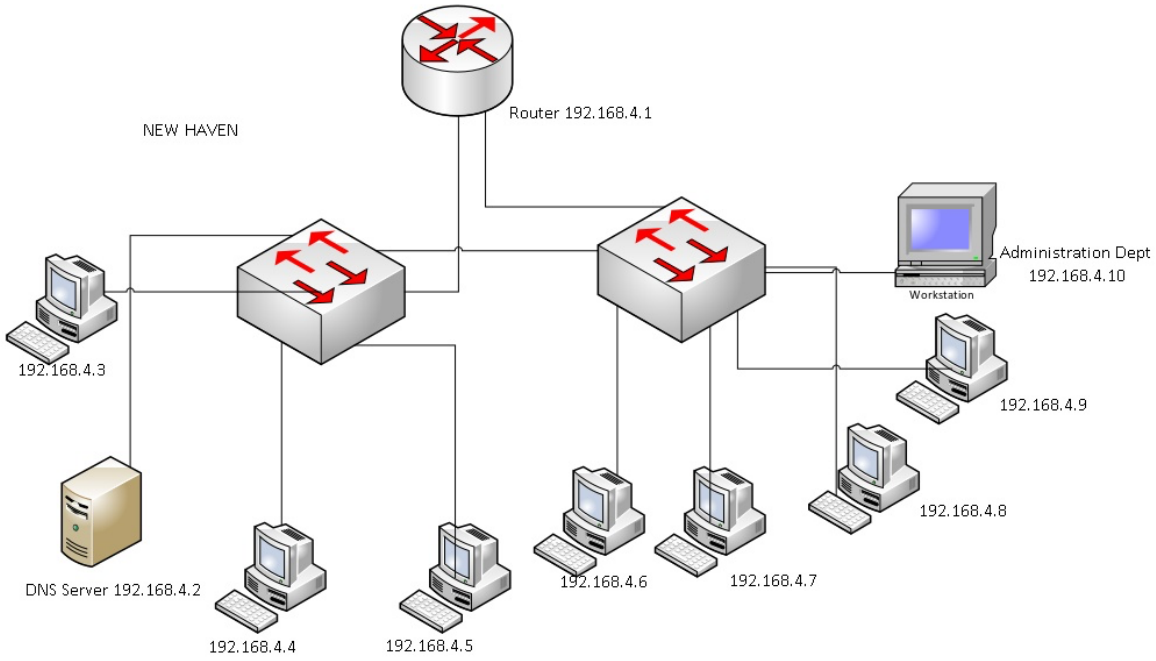
This City is assigned with 192.168.5.0 IP Address Application Server for the entire system. In the Georgia branch we have 2 campuses which are connected to the core layer router. The IP address for Georgia is assigned as 192.168.5.0. The network 192.168.5.1 is assigned as default gateway or router address and 192.168.5.2 is assigned with the server. Rest all the addresses from 192.168.5.3 -192.168.5.254 are addressed to users and client systems working in the Network. DHCP servers are also configured in this branch for the whole network. DHCP server is typically a server that assigns IP addresses automatically for all the devices that are connected to the network. It keeps track of users or devices that are connected to network.

Florida – Network Topology

This City is assigned with 192.168.1.0 IP Address. In the Florida branch we have 1 campus which is connected to the core layer router. The IP address for Florida is assigned as 192.168.1.0. The network 192.168.1.1 is assigned as default gateway or router address and 192.168.1.2 is assigned with the server. Rest all the addresses from 192.168.1.3 -192.168.1.254 are addressed to users and client systems working in the network. Web server is configured in this branch for the whole network. A web server is typically a server that accepts requests via Hyper Text Transfer Protocol (HTTP) and Hyper Text Transfer Protocol Server (HTTPS).

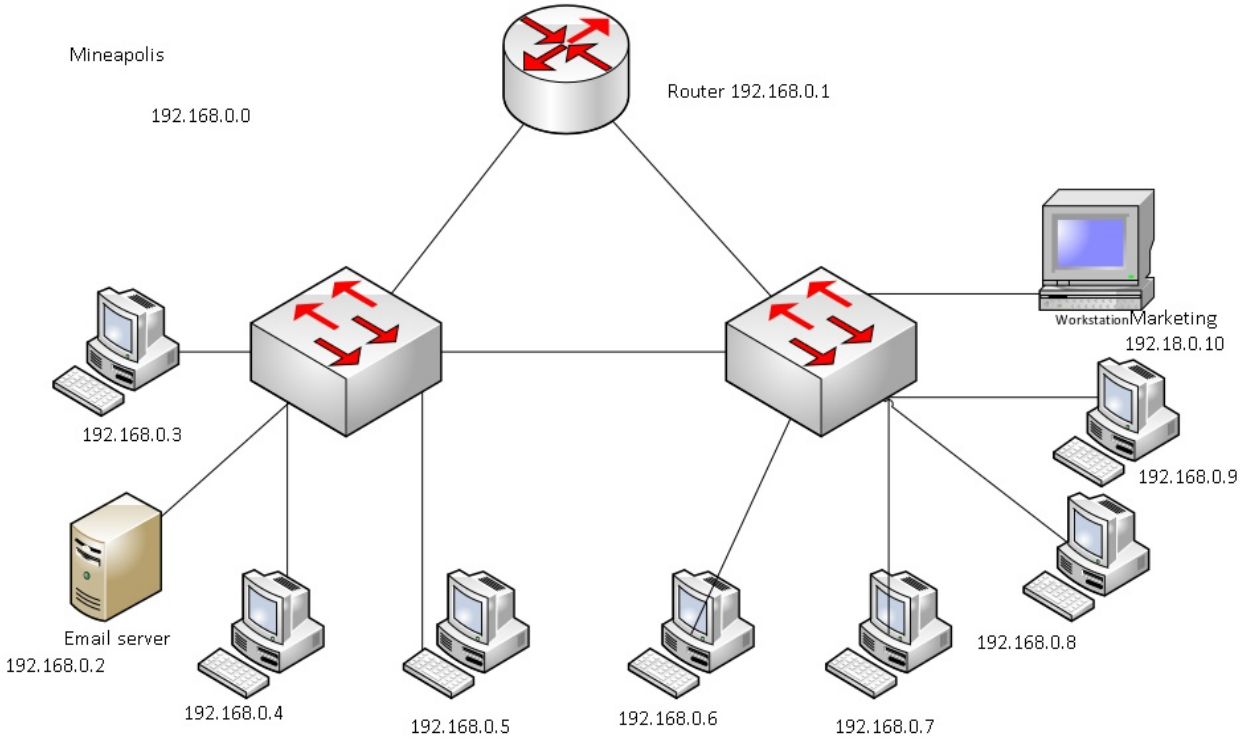


New Haven – Network Topology



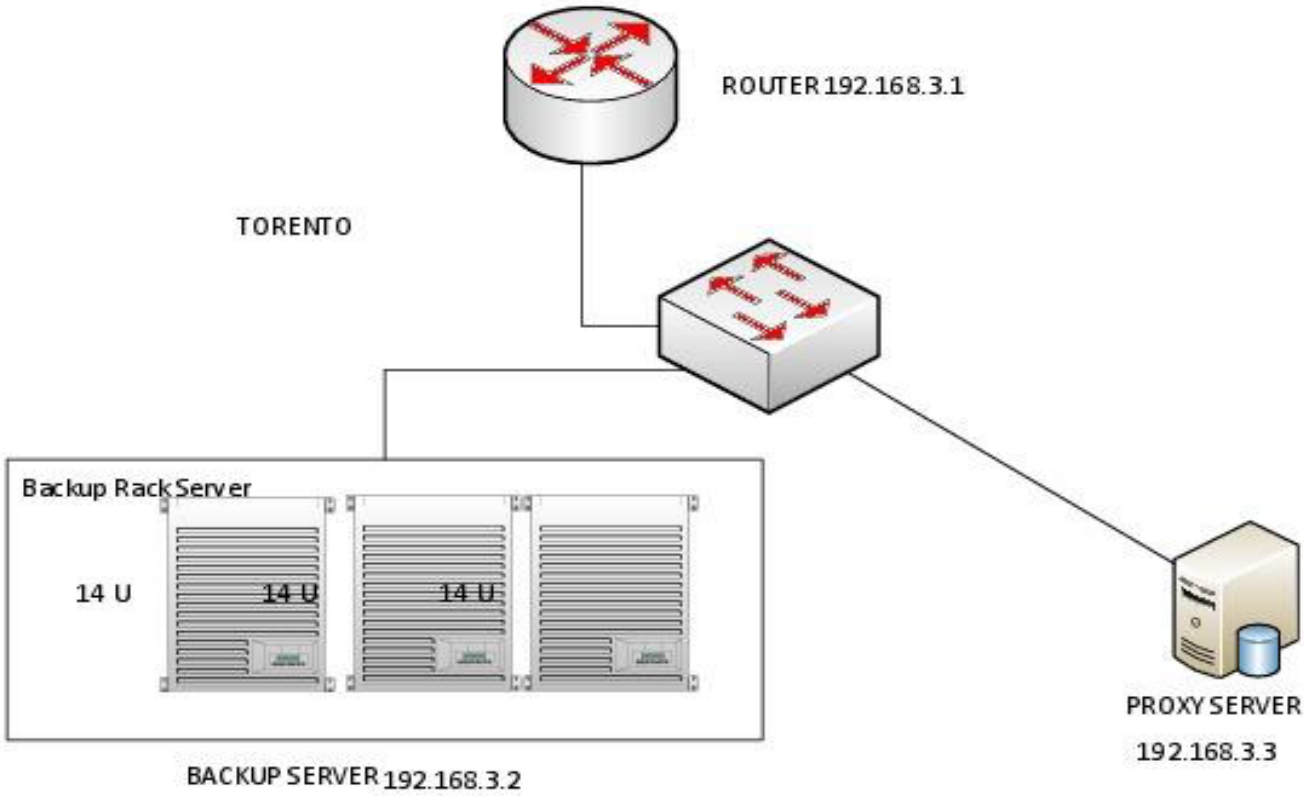
We have assigned 192.168.4.0 as this City address for designing. This City has a DNS server which is assigned to the whole network. The network 192.168.4.1 is assigned as default gateway or router address and 192.168.4.2 is assigned with server. Rest all the addresses from 192.168.4.3 -192.168.4.254 are addressed to users and client systems working in the network. DNS Server assigned here in this network the main purpose of DNS is naming the systems and clients and sub network among the whole network and maintaining the individuality of each branch, department, application, user and subnetwork.

Minneapolis – Network Topology



We have assigned 192.168.0.0 as this City address for designing. This City has an email server which is assigned to the whole network . The network 192.168.0.1 is assigned as default gateway or router address and 192.168.0.2 is assigned with server. Rest all the addresses from 192.168.0.3 -192.168.0.254 are addressed to users and client systems working in the network. Email server is basically a computer system that monitors and works along sending and receiving email to the whole system.

Toronto – Network Topology



This is also assigned as a backup branch and 192.168.3.1 IP address is assigned for this branch. This branch basically acts as a data server which consists of all data together in a backup server. This branch also has a proxy server which acts as mediator for all the incoming and outgoing data. This City has Backup server and Proxy Server which is assigned with the whole network. This city is basically used to store all the data that is evolved in the network on daily basis. The network 192.168.3.1 is assigned as default gateway or router address and 192.168.3.2 is assigned with Backup server and 192.168.3.3 is assigned with Proxy server this is used for data retrieval (If a user needs any data from backup server this works as host). Rest all the addresses from 192.168.5.3 -192.168.5.254 are addressed to users and client systems working in the network.

All these branches also have departments linked together. The main departments we applied for our project are current accounts (given to firms) and saving accounts (given to individuals) - checking account, saving account, money market deposit account (current account in India), certificate of deposit (Fixed Deposit) where these people ask money to invest in credit and saving account.

There will be different departments and with various purposes :

- **Finance Department :** They issue loans (personal, Housing , Business, Education, Mortgage and Vehicle loan).

- **Marketing Department :** They educate people about bank or advertise about bank in the area or place.

- **Administration Department :** There are types in administration department HR, building branches, recruiting employees, infrastructure maintenance. Building operations regarding security.

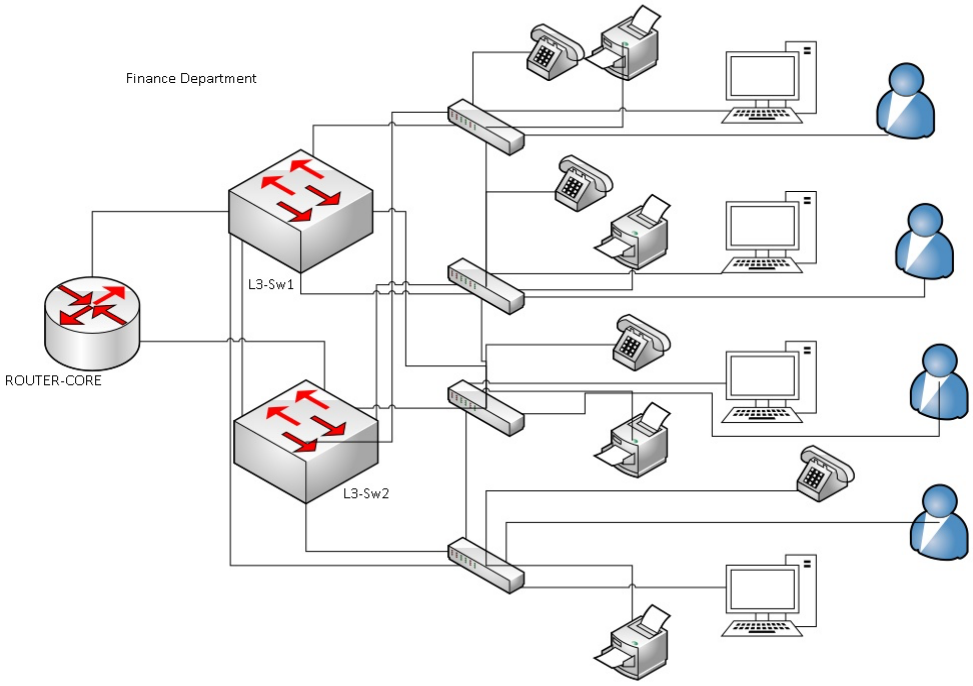
- **Accounting Department :** They check cash maintenance in the bank. That is inflow and outflow of cash and check in the bank and keep track of it. It warns bank if they are going into debt or tell if they're into profits.

- **Sales/Card Department :** ATM, Credit Card, Debit Card, etc.

- **Back office Department :** IT, CRM, Accounting & Finance, Product and Planning.

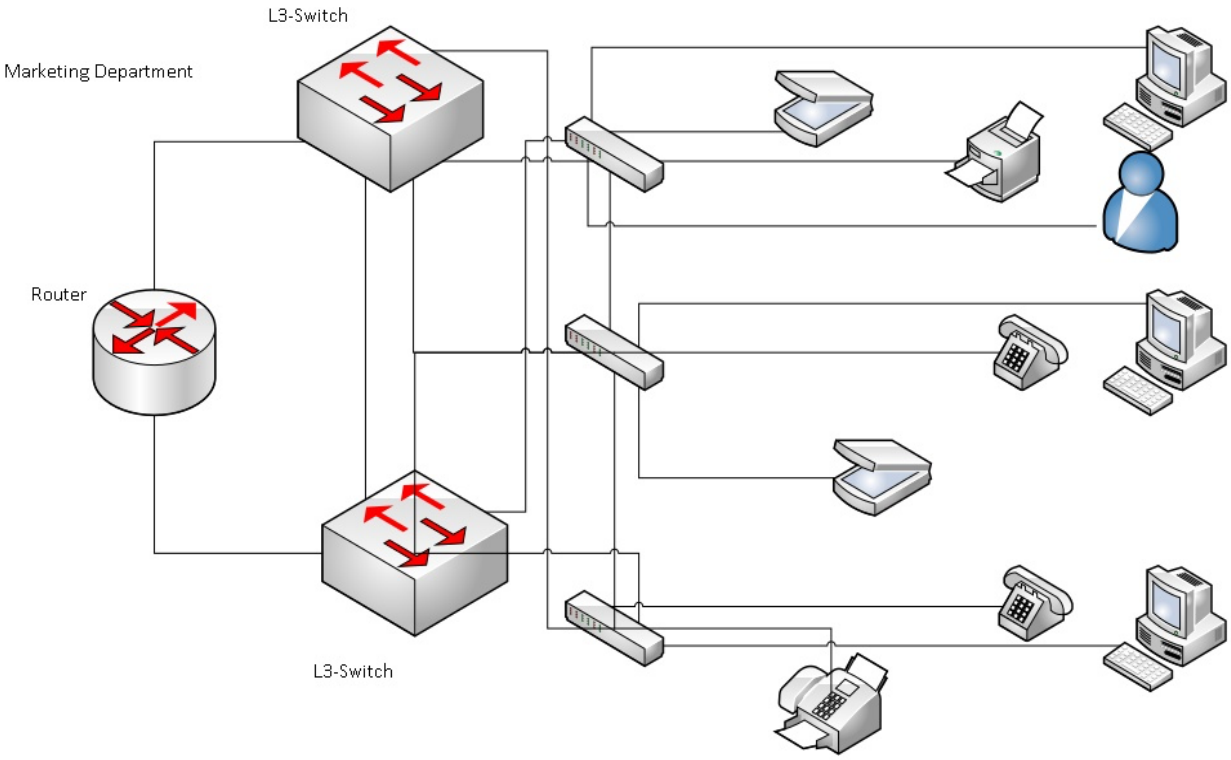
Departmental Requirements :

Financial Department



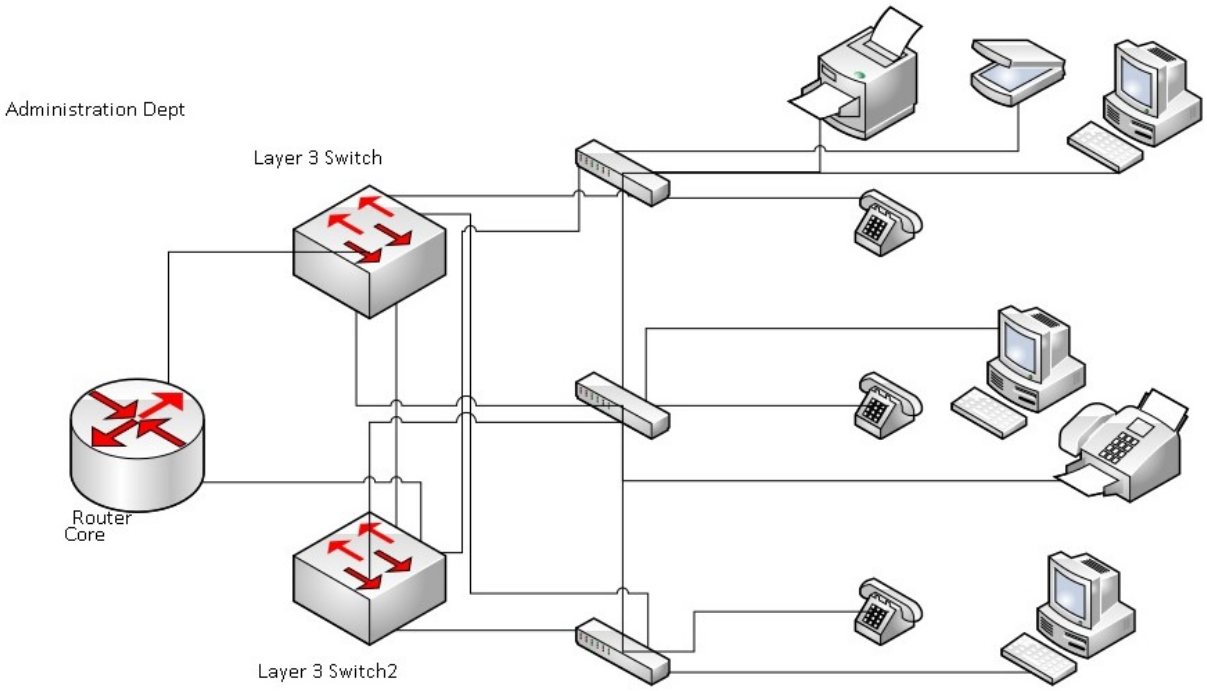
Each user is connected to the core layer router in this department. In this department all the printers, telephones and computers connected are used by the people (users and staff). Checking Account, Saving Account, Money Market Deposit Account (current account in India), Certificate of Deposit (Fixed deposit). These are the 4 types of bank accounts that are issued to people. Checking account is given to people whose age is above 25 and a savings account is given to people below 25 years of age. Money market deposit account is a kind of bank account that is issued only to firms or company's official bank accounts and certificates of deposit are like fixed deposits. Financial department staff ask customers to maintain money in their bank account and with that money these people issue loans and get interest which they pay half to the customer and the other half they use for bank development.

Marketing Department



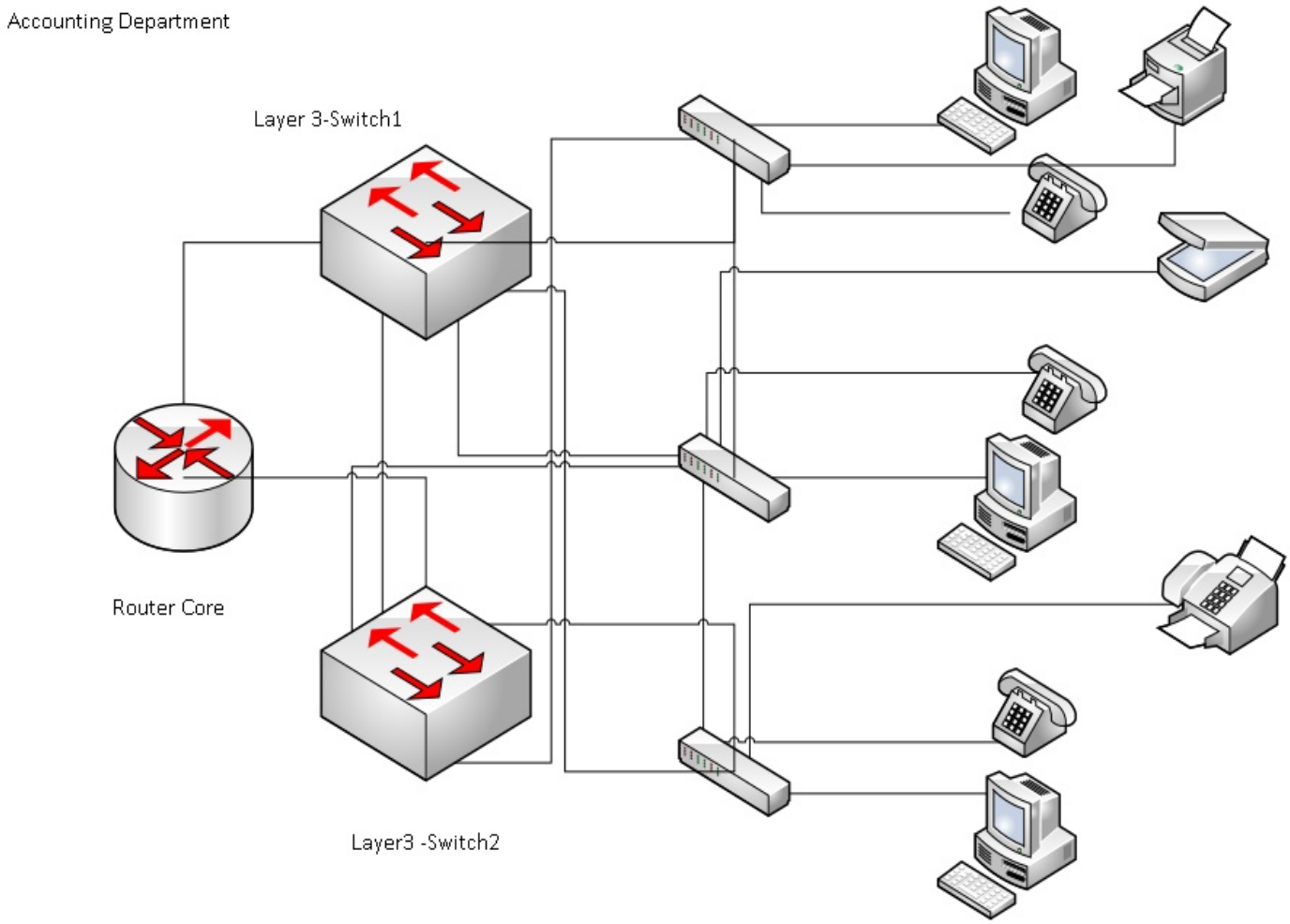
This department all the people are generally engaged in educating people regarding banking and processes involved in banking. These people also deal with the loan process. There are different kinds of loans: Home loan, Vehicle loan, Personal loan, business loan, Education loan, Mortgage loan. These department people advertise about the benefits of taking the loans, interest percentage and process of repaying it.

Administration Department



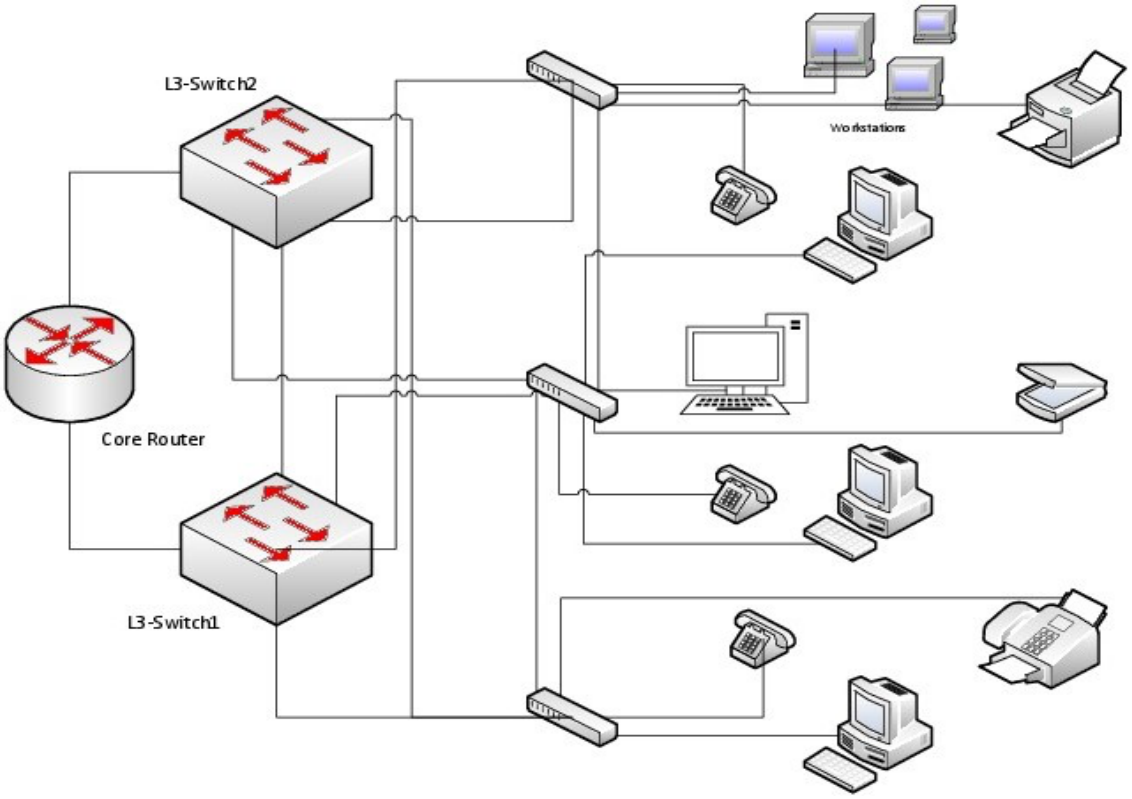
There are types in Administration department which goes like : Human Resources, Building branches, Recruiting employees, Infrastructure maintenance. Building operations are always regarding security. Main work of this administration department is recruiting people and maintaining the human relationships peacefully among the employees. They are also engaged in building infrastructure and operations regarding security maintenance that is maintaining C.C.T.V everywhere around the campus in banks and also, they plan in building new buildings and expanding the infrastructure.

Accounting Department



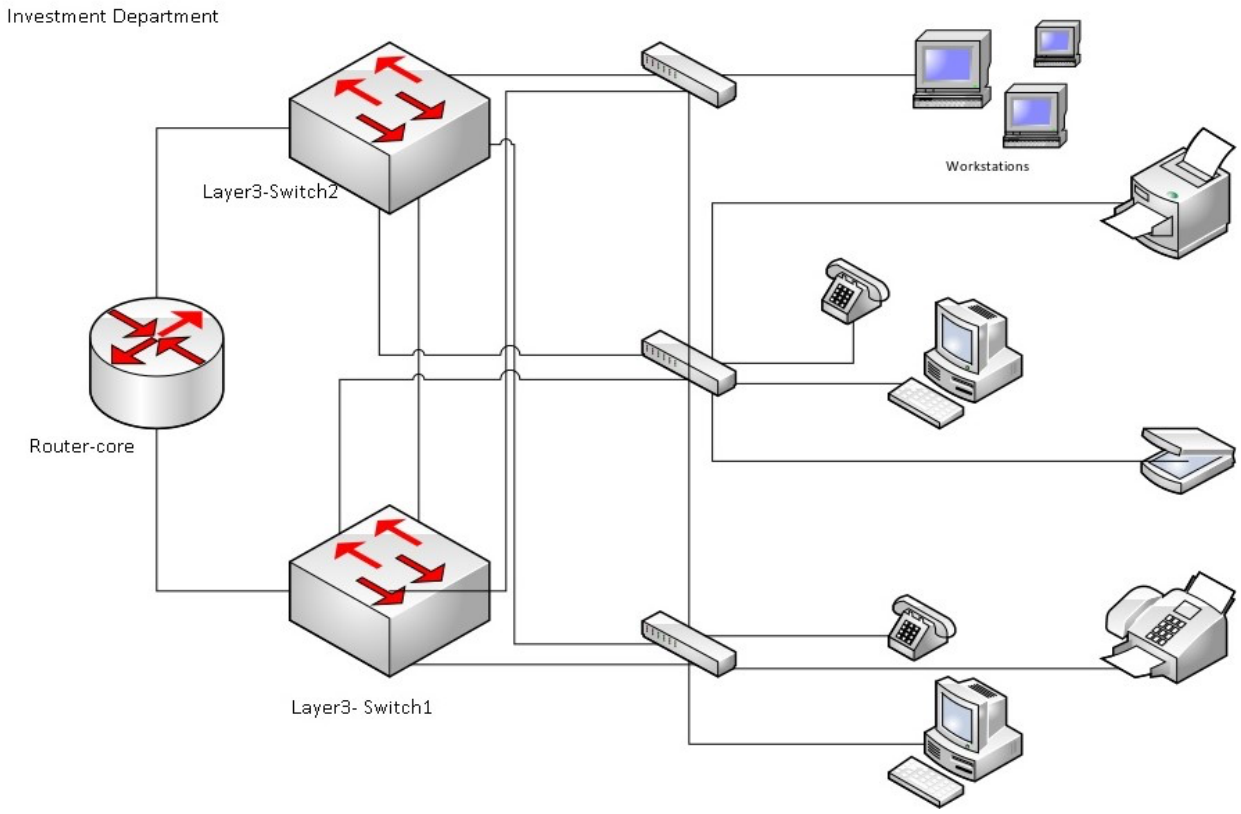
They generally check the cash maintenance in the bank. That is inflow and outflow of cash and check in the bank and keep track of it. It warns the banks if they are going into debt or alerts if they're into profits. This department basically manages the inflow and outflow of the money that is moving in between vendors, users, bank authorities, loan process and all other people working in the network.

Sales/Card Department



In this department it is generally staff working for the bank in the card department that educates people who are eligible for credit card, debit card to take and assists in issuing the card for customers. For repaying the credit card amount that is used by the customer they provide a due date that is usually 30days no interest time after the grace period. Interest will be burdened on the customer; this process is handled and managed by the card department. If you generally take money from an ATM through a credit card there will be charges that will be 10-15% of the amount that has been withdrawn. If there is any fraud that is happening with your transactions this kind of case will also be handled by the card department. So, this department basically covers all the card issuing areas.

Investment Department :



This department handles all the money that is inflowing into the bank and invests that money in any other sector. The main goal or aim of this department is to make money to bank and improve its deposit reserve.

Servers

We mainly used 7 servers in this banking network protocol and 4 other servers in DMZ area. So, totally we have used 11 servers in this prototype and they are :

- Email Server
- Web Server
- DNS Server
- DHCP Server
- Backup Server
- Proxy Server
- Payment Gateway Server
- File Server - Database Server - Printer Server - FTP Server in the DMZ.

- **Email Server :** This server is basically useful for monitoring, screening.

- **Payment Gateway Server :** This is also configured in this branch for the whole network. Payment gateway server is typically a gateway between merchant bank and customer for online banking.

- **Web Server :** This is configured in this branch for the whole network. A web server is typically a server that accepts requests via Hyper Text Transfer Protocol and Hyper Text Transfer Protocol Server.

- **DNS Server :** Server assigned here in this network has the main purpose of DNS - naming the systems and clients and subnetwork among the whole network and maintaining the individuality of each branch, department, application, user and subnetwork.

- **Proxy Server :** This is used for the data retrieval (If a user needs any data from a backup server this works as host).

- **Backup Server :** This is used to store all the data that is evolved in the network on a daily basis.

- **DHCP Server :** This server is used to assign Ip Address to all the users that are present in the network. This is optional but we are using this server in our network.

Security Risks and their Management :

There are Hacked network devices

1) Data can be intercepted, analyzed, altered, or deleted
2) User passwords can be compromised
3) Device configurations can be changed
   - Reconnaissance attacks
   - Denial-of-service attacks

In order to overcome these kinds of attacks we are implementing 12 step security design for our bank network. They are :

- Identify network assets
- Analyze security risks
- Analyze security requirements and tradeoffs
- Develop a security plan
- Define a security policy
- Develop procedures for applying security policies
- Develop a technical implementation strategy
- Achieve buy-in from users, managers, and technical staff
- Train users, managers, and technical staff
- Implement the technical strategy and security procedures
- Test the security and update it if any problems are found
- Maintain security

These are the 12 steps that are implemented by us to protect our network design from a random hacker attack and store our data securely. The basic network assets that we are covering in this security design are : Hardware, Software, Data, Trade, Secrets, Company Reputation, Ledger Balance sheets and financial statements.

Security Plan :

A network security plan is a strategy that specifies the method and procedures used to secure the network from unauthorized users and guards against occurrences that could threaten or undermine the security of a system. It is a high-level document that proposes what an organization is going to do to meet security requirements. Security plan is necessary to secure the infrastructure against unauthorized access, misuse, damage, or loss of company reputation, given the increased threat of hackers constantly exploring the Internet for networks to exploit.

Security Policy :

Network security policy is a written document that lays out the concepts, methods, and standards for enforcing, managing, monitoring, and maintaining network security. Its purpose is to defend the computer network from any act or process that could compromise its security.

A typical security policy generally documents regulations like :

- Rules and approaches to access and modify the network design characteristics.
- Governance and management over internetwork.
- Implementation of the security over the network design mainly on the end user devices to ensure less loss of data.

Security Mechanisms :

These are the techniques for having security services in place. A mechanism may provide a service by itself or in collaboration with others.

Various security mechanisms that are used in the network design to ensure the safety of the data are :

- Physical Security
- Authorization
- Authentication
- Auditing
- Firewall
- Data Encryption
- Packet Filters
- Intrusion Detection and Prevention Systems

Physical Security :

Physical security applies to restricting access to critical network resources by locking them away and protecting them from natural and man-made disasters. Physical security can safeguard a network against inexperienced personnel and contractors misusing network equipment inadvertently. It can also defend the network from walk-in hackers, competitors, and terrorists who change equipment configurations.

Authentication :

Authentication establishes the identity of the person requesting network services. Although it can also refer to authenticating equipment or software processes. Some routing protocols, for example, enable route authentication, which requires a router to meet certain requirements before another router accepts its routing changes.

Authentication basically depends on three important factors :

- Something the user has
- Something the user knows
- Something the user is

Authorization :

Authentication determines who has access to network resources; authorization determines what they can do once they have. Processes and users are granted privileges through authorization. A security administrator can control elements of a network via authorization.

Data Encryption :

Encryption fumbles data to prevent it from being read by anybody other than the intended recipient. Before sending data over a network, an encryption device encrypts it. Before delivering data to an application, a decryption device decrypts it. An encryption or decryption device can be a router, server, end system, or dedicated device. Ciphered data is data that has been encrypted. Plain text refers to data that is not encrypted. The purpose of encryption is to ensure that even if the technique is known, an intruder cannot decipher the communication without the necessary key. A secret key is the name for this type of key. A symmetric key is one in which both the sender and the recipient utilize the same secret key. A symmetric key system is well known as the Data Encryption Standard.

Packet Filters :

On routers, firewalls, and servers, packet filters can be configured to accept or reject packets from specific addresses or services. Authentication and authorization mechanisms are augmented by packet filters. They aid in the prevention of illegal access, theft, destruction, and DoS attacks on network resources.

Firewalls :

A firewall uses rules to determine which traffic should be allowed or refused. A static stateless packet-filter firewall examines individual packets and is designed for speed and ease of configuration. A stateful firewall can keep track of communication sessions and accept or prohibit traffic more intelligently. A stateful firewall, for example, can remember that a protected client requested data from an Internet server and then allow data back in for that connection. A proxy firewall is another form of firewall. Proxy firewalls are the most advanced but also the least prevalent type of firewall. A proxy firewall works as a go-between for hosts, intercepting some or all application traffic between local clients and external servers. Proxy firewalls inspect packets and enable stateful session tracking. These firewalls are capable of blocking harmful communications as well as content that is deemed inappropriate.

Intrusion Detection and Prevention Systems :

An intrusion detection system identifies malicious occurrences and notifies an administrator of the occurrence via email, paging, or logging. Statistics and anomaly analysis are also possible with an IDS. Some IDS devices can send data to a central database that combines data from many sensors to offer a network administrator a complete picture of the network's security in real time. By applying regulations to a firewall or configuring it to inspect traffic as it enters the firewall, an intrusion prevention system can dynamically prohibit traffic. An IDS that can detect and mitigate attacks is known as an IPS.

Phase 3

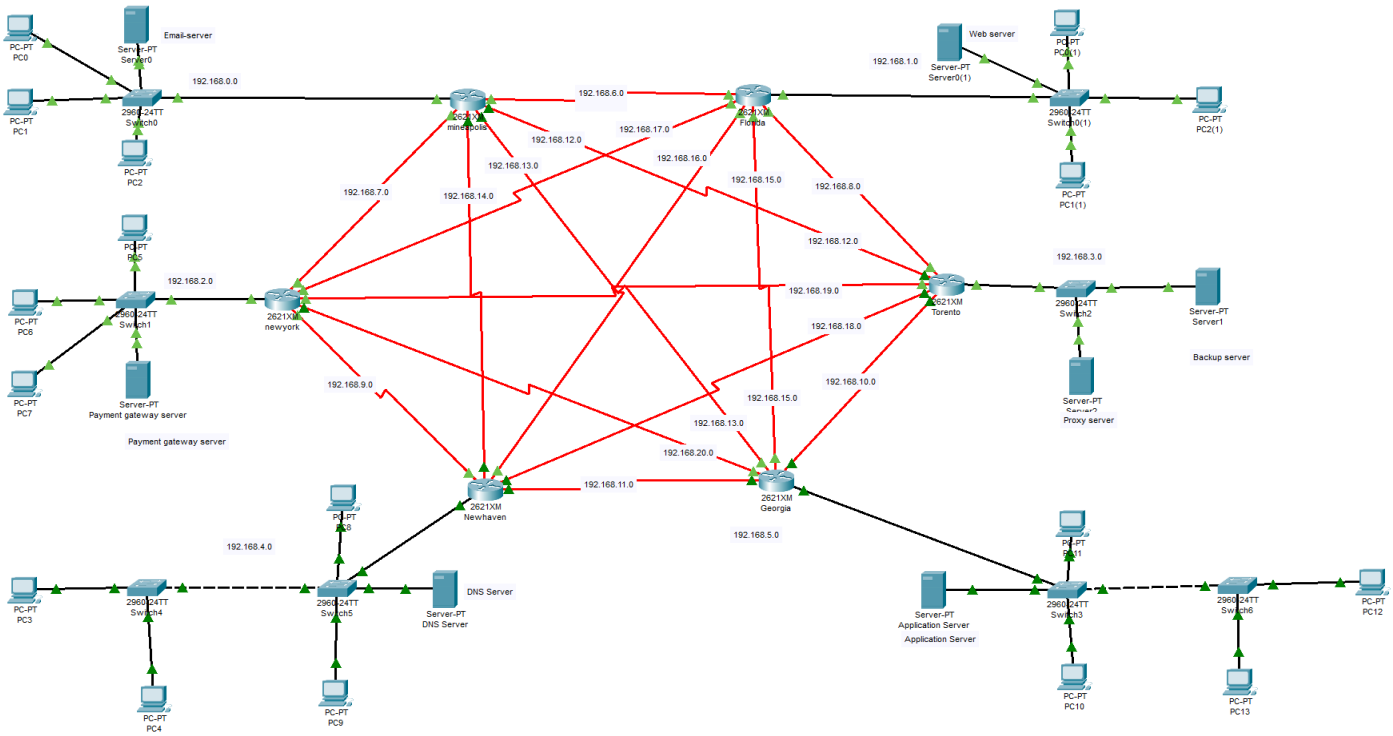
Physical Design

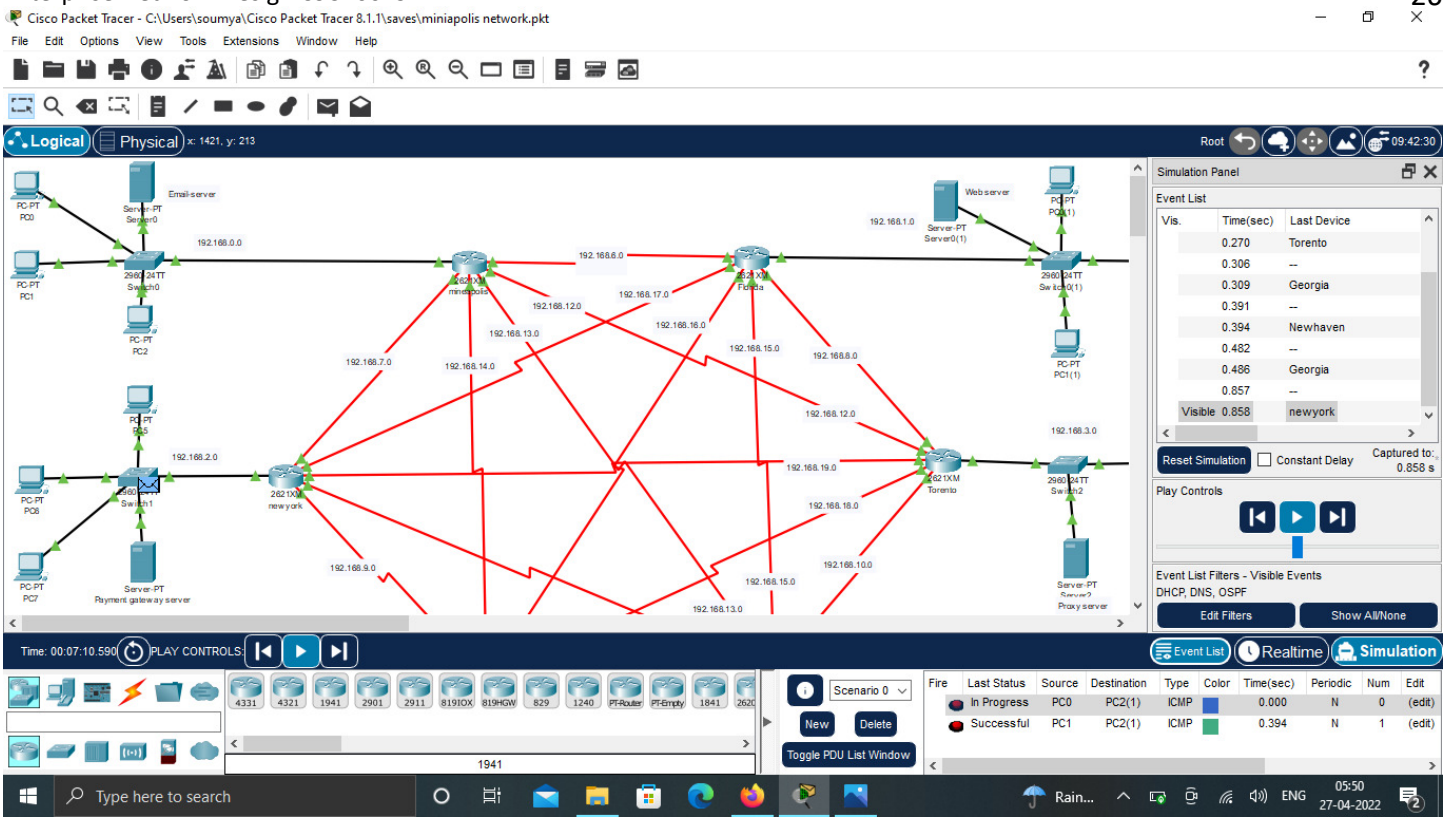
Implementation – Cisco Packet Tracer :

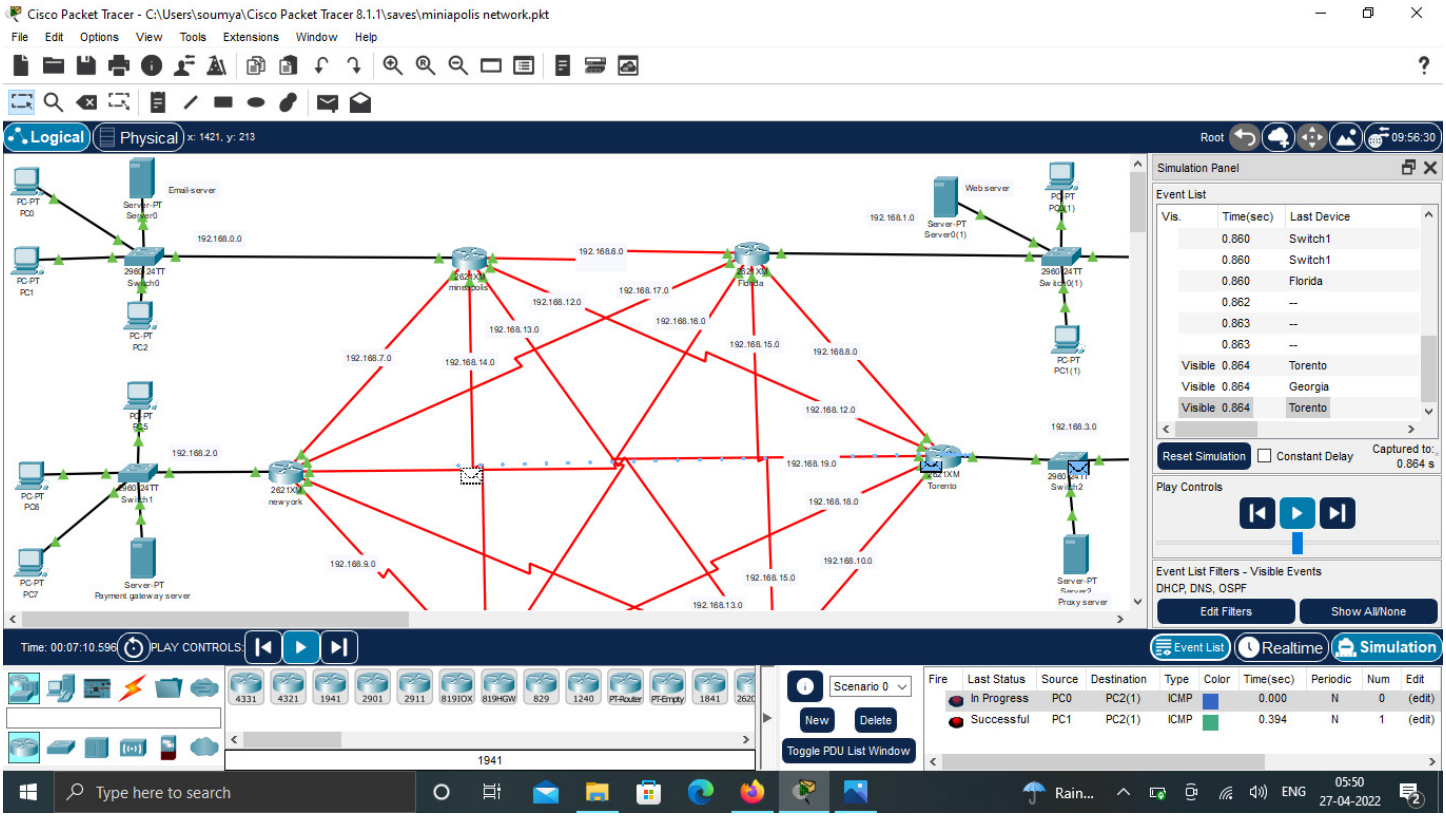
For implementing this bank prototype we have used 2621XM routers which have 8 serial ports, So that it will be easy for us to connect to 6 cities and we have also used 2960-24TT switches all over the network to connect to various campuses among the cities which are then interconnected to the servers and users. All the serial ports are assigned with IP addresses so they can be recognized between the cities without confusion.

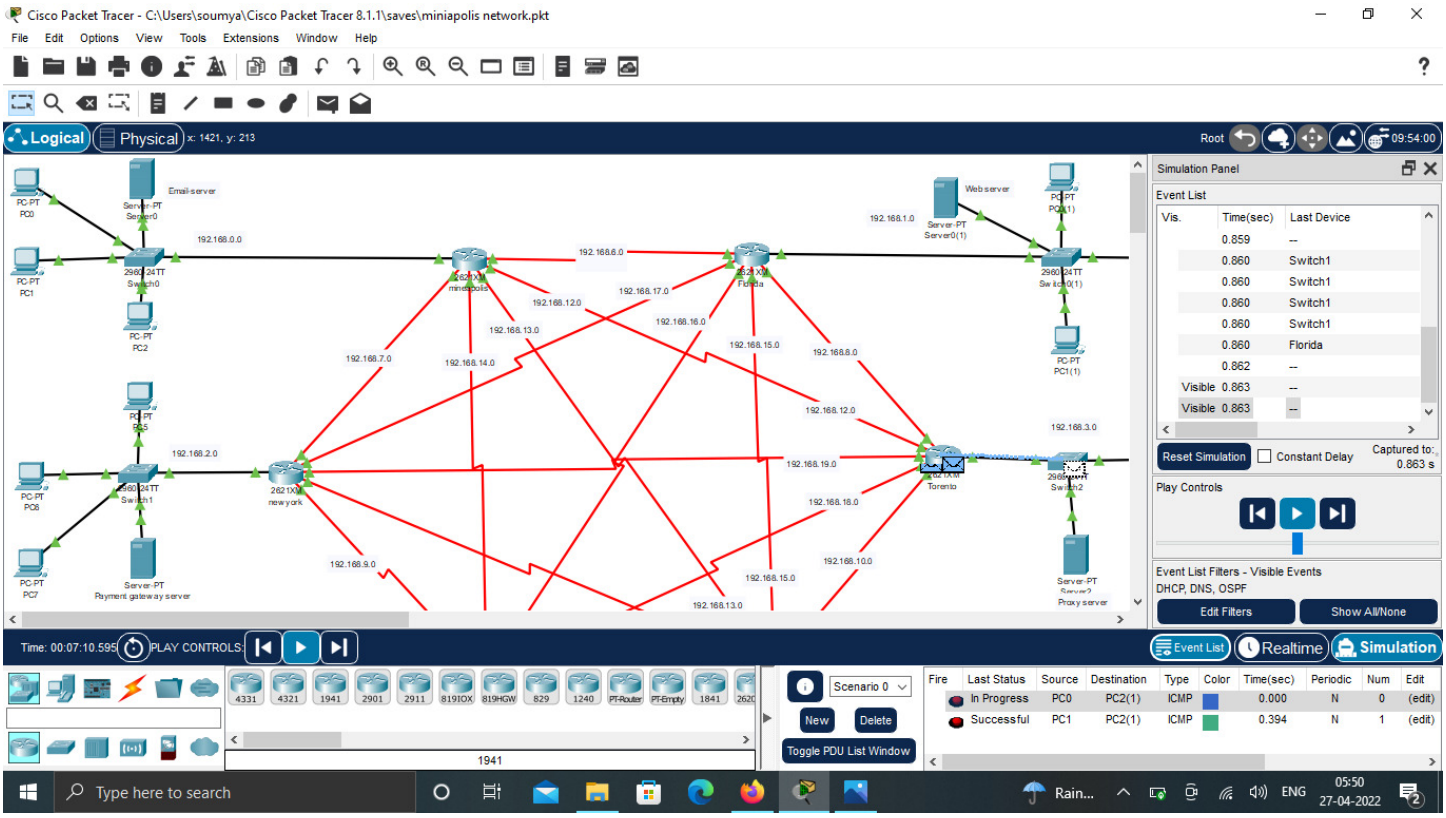
Cisco Packet Tracer :

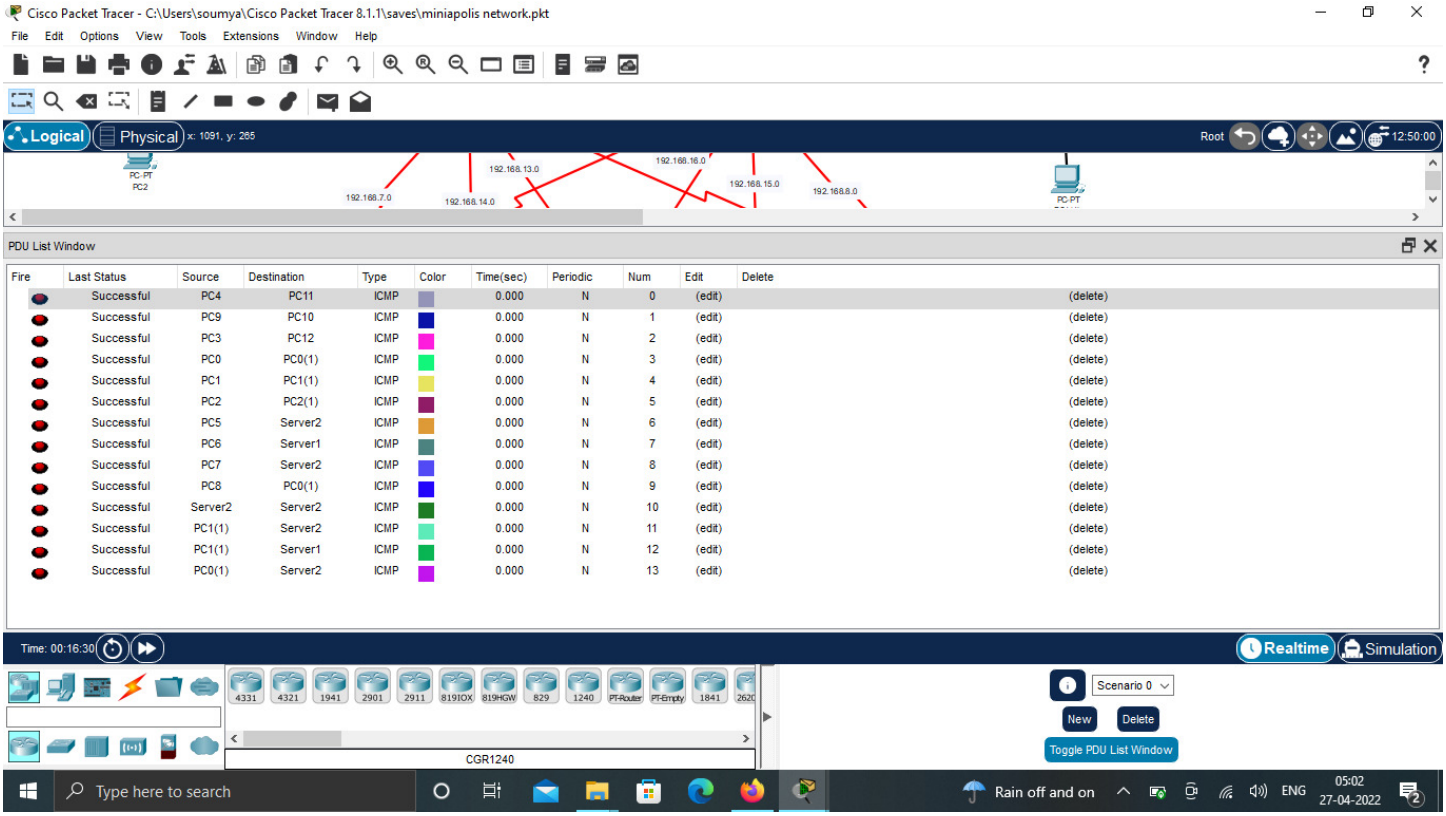
- Cisco Packet Tracer is a visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks.
- Using packet tracer we have implemented network topology, assigned routers and switches.
- We can also configure each and every router and network with the IP address and tested whether the data transfer is successful or not.

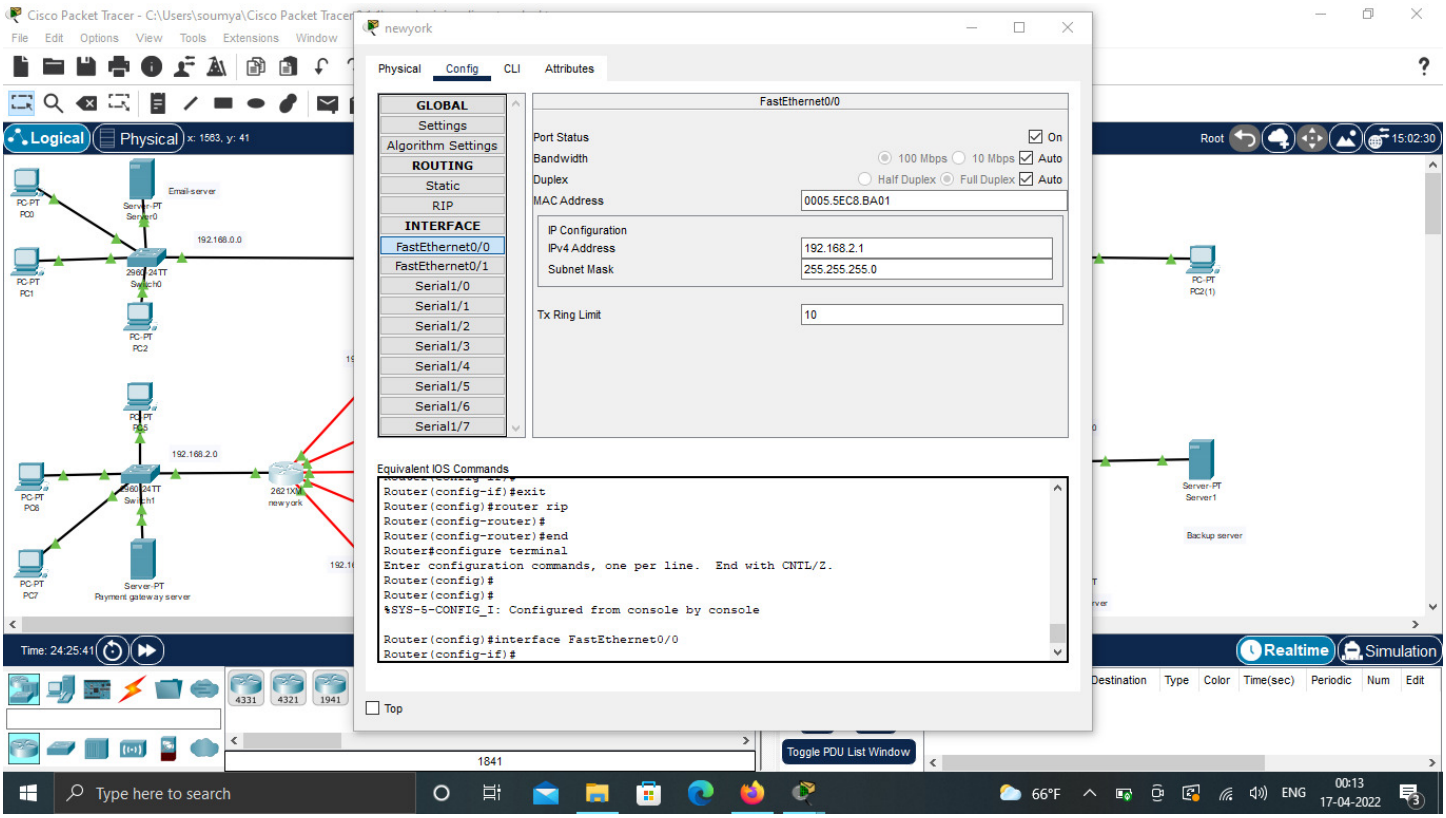



Cisco Packet Tracer - C:\Users\soumya\Cisco Packet Tracer 8.1.1\saves\miniapolis network.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 1421, y: 213
Root 09:42:30
Simulation Panel
Event List
Vis. Time(sec) Last Device
0.270 Torento
0.306 --
0.309 Georgia
0.391 --
0.394 Newhaven
0.482 --
0.486 Georgia
0.857 --
Visible 0.858 newyork
Reset Simulation Constant Delay Captured to: 0.858 s
Play Controls
Event List Filters - Visible Events
DHCP, DNS, OSPF
Edit Filters Show All/None
Time: 00:07:10.590 PLAY CONTROLS:
Event List Realtime Simulation
Scenario 0 New Delete Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit
In Progress PC0 PC2(1) ICMP 0.000 N 0 (edit)
Successful PC1 PC2(1) ICMP 0.394 N 1 (edit)
1941
Type here to search
Rain... ENG 05:50 27-04-2022


Cisco Packet Tracer - C:\Users\soumya\Cisco Packet Tracer 8.1.1\saves\miniapolis network.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 1421, y: 213
Root 09:56:30
Simulation Panel
Event List
Vis. Time(sec) Last Device
0.860 Switch1
0.860 Switch1
0.860 Florida
0.862 --
0.863 --
0.863 --
Visible 0.864 Torento
Visible 0.864 Georgia
Visible 0.864 Torento
Reset Simulation Constant Delay Captured to: 0.864 s
Play Controls
Event List Filters - Visible Events
DHCP, DNS, OSPF
Edit Filters Show All/None
Time: 00:07:10.596 PLAY CONTROLS:
Event List Realtime Simulation
Scenario 0 New Delete Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit
In Progress PC0 PC2(1) ICMP 0.000 N 0 (edit)
Successful PC1 PC2(1) ICMP 0.394 N 1 (edit)
1941
Type here to search
Rain... ENG 05:50 27-04-2022


Cisco Packet Tracer - C:\Users\soumya\Cisco Packet Tracer 8.1.1\saves\miniapolis network.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical
Simulation Panel
Event List
Reset Simulation
Constant Delay
Play Controls
Event List Filters - Visible Events
DHCP, DNS, OSPF
Edit Filters
Show All/None
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Type here to search
Rain...
ENG
05:50
27-04-2022


Cisco Packet Tracer - C:\Users\soumya\Cisco Packet Tracer 8.1.1\saves\miniapolis network.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical
PDU List Window
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Type here to search
Rain off and on
ENG
05:02
27-04-2022

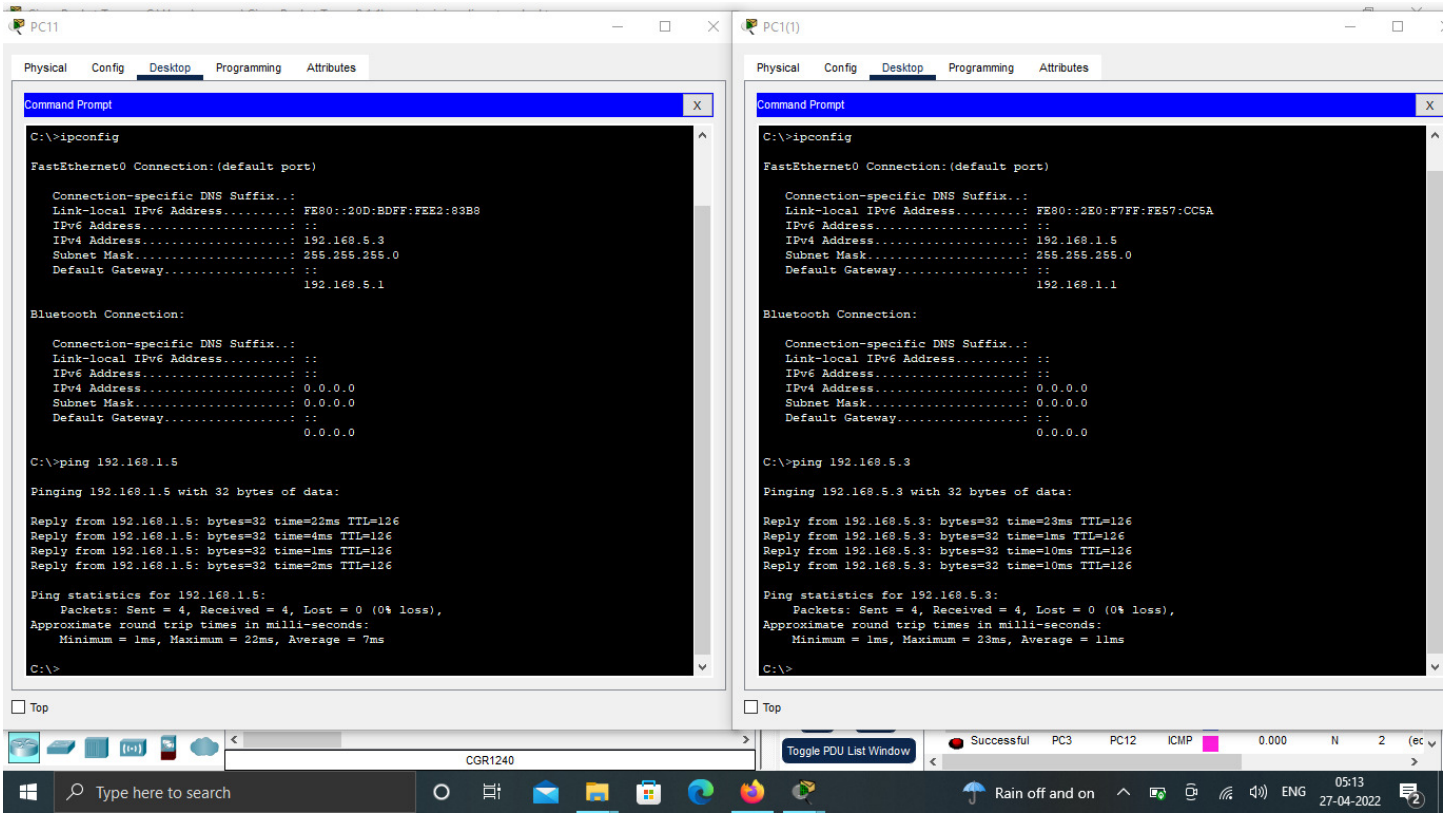


We have manually checked if the network between each user in the city is connected to one other.

This is done individually with testing from one city device to other city devices instead of buffer manager interface. After testing this manually buffer tesing is implemented and checked.

Ping from a PC to Another PC :

- The above screenshot shows the successful implementation of the connection across two different systems, where it executes perfectly.
- All the data packets are received without any loss of data.



Phase 4

Testing/Optimization/Documentation

Why testing is important ?

- We should always verify whether the design meets the business goals and technical goals for the network that is desired by the clients.
- There is a strict validation required for LAN and WAN selections depending upon the requirements of the network design.
- Should verify if there are any connectivity throughout the network design.
- Testing should also help as they are the deciding factor to select the correct optimizing technique which is the next step after testing.

Scope

- We can say that it is not at all practical for us to implement a full-scale network design, So we will be designing a prototype design only.
- Testing helps to verify all the important capabilities that might not perform inadequately.
- Complex, sophisticated functions and functions driven by the need to make tradeoffs are examples of risky functions.

Types of Tests

- Application Response-Time Testing
- Throughput Testing
- Availability Testing
- Regression Testing

Application Response-Time Testing :
Response Time Testing determines how quickly one system node responds to another's request. It is the time it takes for a system to get to a given input and complete the process.

Throughput Testing :
The number of packets that successfully arrive at their destinations is measured by throughput. Throughput capacity is usually expressed in bits per second, although it can alternatively be expressed as data per second. Packet arrival is critical for high-performance network service. Testing throughput for a given network is very crucial for the design.

Availability Testing :
Availability testing, also known as Durability testing, is a type of performance testing in which the application is run for a specified length of time, failure events and repair times are collected, and the availability percentage is compared to the service level agreement.

Regression Testing :
Regression Testing is a type of testing that is used to test the modification which result in the issues in the network design. This is nothing but a full or partial selection of already issues found which are re-executed to ensure existing network design work fine.

What is Optimization ?

Network optimization's main goal is to achieve the greatest possible network design and performance at the lowest possible cost. The network must promote enhanced productivity and usability while also allowing for effective and efficient data transmission.

Why Optimization is important ?

- Optimization is crucial to meet the business and technical goals as it increases the productivity and usability of the network design.
- It enables the network to use the bandwidth efficiently.
- Because of optimization, the network can be able to meet the quality-of-service requirements.

IP Multicast :

IP multicast is a means of transmitting datagrams via the Internet Protocol (IP) to a group of interested recipients in a single transmission. It is a type of multicast that is special to IP and is used for streaming media and other network applications. With IP multicast, you can send a high-volume multimedia stream just once instead of once for each user.

- Multicast Addressing
- Multicast Registration
- Multicast Routing Protocols

Multicast Addressing :

A multicast address designates a group of hosts that share the same IP address. A device does not receive multicast addresses; instead, it listens for and receives traffic destined for a multicast group that it has joined through some mechanism.

Internet Group Management Protocol (IGMP) :

This is a mechanism that lets multiple devices to share the same IP address and hence receive the same data. IGMP is a network layer protocol that enables multicasting on Internet Protocol version 4 networks (IPv4). Host transmits a membership-report message to inform routers on the segment that traffic for a group should be multicast to the host's segment. When computers and other networked devices seek to join a multicast group, they use IGMP. A router that supports IGMP waits for IGMP messages from devices to determine which multicast groups they belong to.

Multicast Routing Protocols :

In contrast to unicast routing, which delivers 1: 1 essential data, multicast routing sends a single message to all subscribers in a group. Multicast transmission requires the use of the IGMP protocol and the multicast routing protocol for registration subscriber grouping and control traffic.

Why Documentation is Important ?

The hardware, software, servers, directory structure, data, and how it all works together are all documented in network documentation. Any information that aids network design in keeping the network up and operating should be included in network documentation. This data can be presented in any format desired.

Documentation considerations :

- A network topology for the new design
- Information on the protocols, technologies, and products that form the design
- An implementation plan
- A training plan
- Support and service information
- Prices and payment options
- Qualifications of the responding vendor or supplier
- Recommendations from other customers
- Legal contractual terms and conditions

References

- https://canvas.newhaven.edu/courses/12845/modules
- https://www.comparitech.com/net-admin/routing- protocol-types-guide/
- https://www.ccexpert.us/network-design-2/characterizing-types-of-traffic-flow-for-new-network- applications.html
- https://en.wikipedia.org/wiki/Chase_Bank
- https://www.netacad.com/courses/packet-tracer
- https://blog.gigamon.com/2021/11/15/network-optimization/