COMPUTER NETWORKS

Case Study

<<Bank System Network>>

Group Number:16

Registration No	Name	Email ID	Contribution
CB.EN.U4CSE21322	JASWANTH G	cb.en.u4cse21322@cb.students.amrita.edu	FIRST FLOOR
CB.EN.U4CSE21328	K.ABHISHEK	cb.en.u4cse21328@cb.students.amrita.edu	FOURTH FLOOR
CB.EN.U4CSE21329	K.HITEESH RAJU	cb.en.u4cse21329@cb.students.amrita.edu	THIRD FLOOR
CB.EN.U4CSE21361	SV SAI SATYA	cb.en.u4cse21361@cb.students.amrita.edu	SECOND FLOOR

Why Networking is required for the application:

1. Remote access and convenience
2. Real-time Transactions
3. Data Synchronization
4. Security and Authentication
5. Integrity with third party services
6. Updates and Maintenance
7. Communication with ATM's and Point of Sales(POS) systems
8. Customer Support and Communication

Case study on Rockers Company Ltd:

First Floor			
No.	**Departments**	**No. of PC**	**No. of Printers**
1	Management	20	4
2	Research	20	4
3	Human resource	20	4

Second Floor			
No.	**Departments**	**No. of PC**	**No. of Printers**
1	Marketing	20	4
2	Accounting	20	4
3	Finance	20	4

Third Floor			
No.	**Departments**	**No. of PC**	**No. of Printers**
1	Logistics and store	20	4
2	Customer care	20	4
3	Guest Area	40	2

Fourth Floor				
No.	**Departments**	**No. of PC**	**No. of Printers**	**No of Servers**
1	Administration	20	2	
2	ICT	20	2	
3	Server Room	2 Admin PCs		3 (DHCP, HTTP and Email)

Problem statement:

Rockers Company Ltd. is a US-owned company that deals with Banking and Insurance. The company is intending to expand its services across the African continent having the first branch to be located in Nairobi, Kenya. The company has secured a four-story building to operate within the Kenyan capital city. Therefore, the company would like to allow sourcing the knowledge from a group of final-year students from the local university to design and implement their company network. Assume you are among the students to take over this role, carefully read down the requirements then model the design and implement the network based on the company's needs.

Requirements:

Use any of the following network simulation software to implement the above topology.

- Simulation software: Cisco Packet tracer or GNS3 for design and implementation.

Use OSPF as the routing protocol to advertise routes.

Each department is required to have a wireless network for the users.

Each department except the server room will be anticipated to have around 60 users both wired and wireless users.

Host devices in the network are required to obtain IPv4 addresses automatically.

Devices in all the departments are required to communicate with each other.

Create HTTP, and E-mail servers.

All devices in the network are expected to obtain an IP address dynamically from the dedicated DHCP servers located at the server room.

Configure SSH in all the routers for remote login.

Configure the basic configuration of the devices: Hostnames, Line Console and Enable passwords, Banner messages Disable domain IP lookup, encrypt all configured passwords.

Each department should be in a different VLAN and subnetwork; VLANs you will use in your case, e.g. 10, 20, 30… etc..

Planning of IP Addresses: You have been given 192.168.10.0 as the base address for this network. Do subnetting based on the number of hosts in every department as provided above. Identify subnet mask, useable IP address range, and broadcast address for each subnet.

End Device Configurations: Configure all the end devices in the network with the appropriate IP address based on the calculations above.

Configure port-security: Use sticky command to obtain MAC Address and Violation mode of the shutdown.

Test and Verifying Network Communication.

How WiFi works in Banking Network?

- Each department will have its own wireless network to cater to around 60 users.
- You will need to implement wireless access points (WAPs) strategically within each department to provide adequate coverage.
- Each wireless network should be configured with a unique Service Set Identifier (SSID) to differentiate between departments.

- Security mechanisms such as WPA2 or WPA3 should be implemented to secure the wireless networks. Consider using strong encryption protocols and complex pre-shared keys

Benefits of computer networks in Banking:

- Improved Communication
- Resource Sharing
- Wireless Connectivity
- Security and Access Control
- Centralized Management

Protocols in Banking Network:

- HTTPS (Hypertext Transfer Protocol Secure)
- SSL/TLS (Secure Sockets Layer/Transport Layer Security)
- FTPS (File Transfer Protocol Secure)
- SFTP (Secure File Transfer Protocol)

Software/Operating System used:

1) Operating System:

a) Core banking systems:

i) IBM z/OS

ii) Microsoft Windows Server

iii) Linux (RedHat and SUSE)

b) ATMs (Automated Teller Machines):

i) Microsoft Windows Embedded

ii) Linux (Customized distributions)

2) Database Management Systems (DBMS):

a) Oracle Database

b) IBM Db2

c) Microsoft SQL Server

3) Transaction Processing Systems:

a) CICS (Customer Information Control System) on IBM mainframes

b) ACI Worldwide's BASE24

4) Internet Banking/ Web Services:

a) Java EE (Enterprise edition)

b) .NET framework

c) Apache Tomcat

5) Security Systems:

a) Encryption and decryption tools

b) Anti-fraud systems

c) Firewalls and Intrusion Detection Systems (IDS)

6) Cloud Services:

a) Banks may use cloud services, often with a focus on private or hybrid clouds to ensure security and compliance.

PROGRAMMING LANGUAGES:

1) Mainframe Development:

a) Cobal

b) PL/I(Programming Language 1One)

c) Assembler for the target mainframe architecture (e.g., IBM Assembler)

2) Web and Application Development:

a) Java

b) C#

c) Python

d) JavaScript

3) Database Query Languages:

a) SQL (Structured Query Language)

HARDWARE/ DEVICES USED:

1) Servers:

a) IBM zSeries mainframes

b) x86-based servers for distributed systems

2) ATM's:

a) Various manufacturers with embedded systems running specialized software on Windows or Linux.

3) Networking devices:

a) Routers and switches for internal network communication

b) Firewalls for security

c) Intrusion Prevention Systems (IPS)

4) Banking Systems:

a) Core Banking Servers

b) ATM Control Systems

c) Online Banking Servers

5) Security Devices:

a) Hardware Security Modules (HSMs) for key management

b) Biometric authentication devices

6) Data Storage:

a) SAN (Storage Area Network) and NAS (Network Attached Storage) systems for data storage and retrieval.

Why measure network performance?

Measuring network performance in the context of a banking network is particularly critical due to the sensitive nature of financial transactions and the high demand for seamless and secure services. Here are specific reasons why measuring network performance is essential for a banking network:

Transaction Speed and Responsiveness:

Reason: Customers expect fast and responsive banking services.

Impact: Slow transaction processing can lead to customer dissatisfaction and impact the overall user experience.

Data Security and Integrity:

Reason: Banking networks handle sensitive customer data and financial transactions.

Impact: Poor network performance may increase the risk of data breaches or unauthorized access, compromising the security and integrity of customer information.

Reliability of Online Banking Services:

Reason: Online banking heavily relies on network connectivity.

Impact: Unreliable network performance can lead to service outages, preventing customers from accessing their accounts, making transactions, or using other online banking services.

Compliance with Regulatory Standards:

Reason: Financial institutions must comply with strict regulatory standards.

Impact: Inadequate network performance may lead to non-compliance with regulations, resulting in legal consequences and reputational damage.

Fraud Detection and Prevention:

Reason: Timely processing and analysis of transactions are crucial for fraud detection.

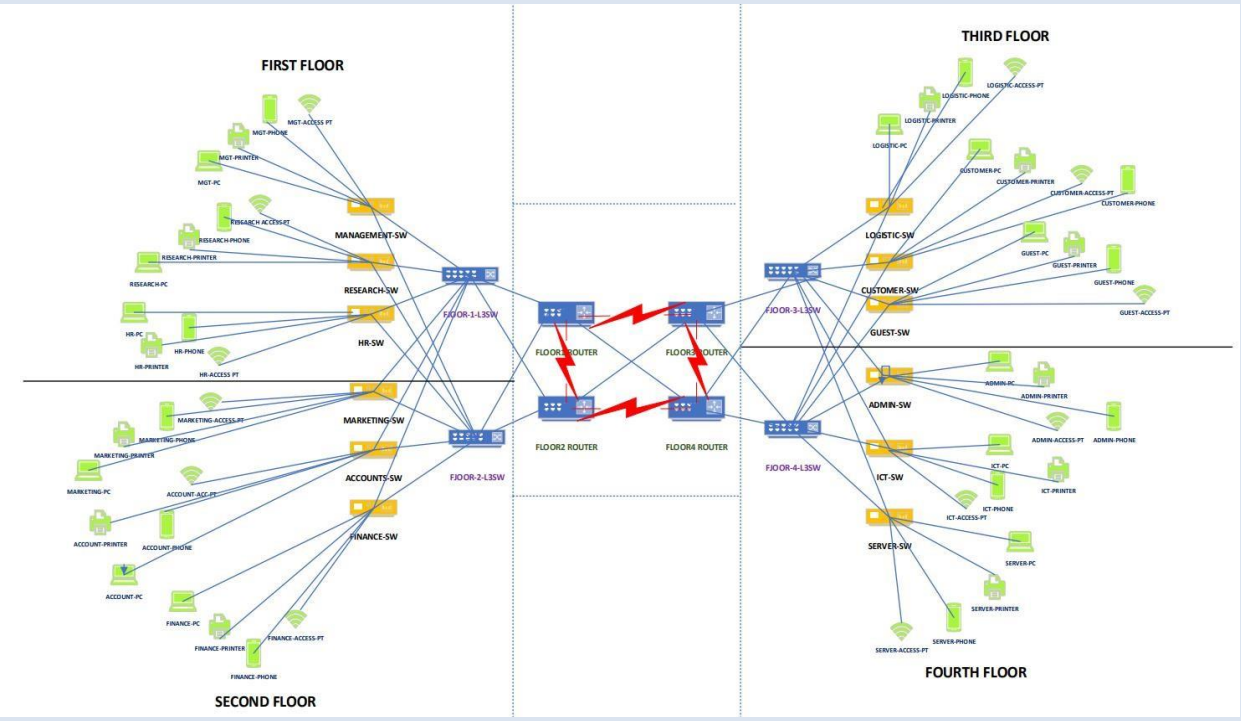
Impact: Network latency or downtime can hinder real-time monitoring and increase the risk of fraudulent activities going unnoticed.

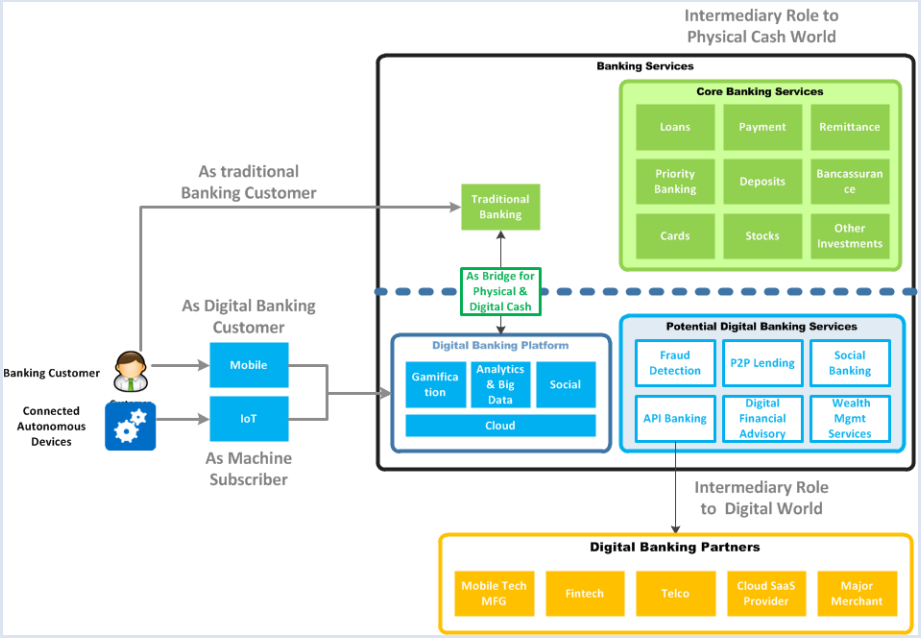
Performance parameters:

Parameter	Meaning	Formula
Bandwidth	Bandwidth is the capacity of a wired or wireless network communications link to transmit the maximum amount of data from one point to another over a computer network or internet connection in a given amount of time	Expressed as bits per second (bps), modern network links have greater capacity, which is typically measured in millions of bits per second (megabits per second, or Mbps) or billions of bits per second (gigabits per second, or Gbps).
Throughput	Throughput measures the percentage of data packets that are successfully being sent; a low throughput means there are a lot of failed or dropped packets that need to be sent again.	
Packet Loss	Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination.Due to network congestion	Efficiency = 100% * (transferred - retransmitted) / transferred Network Loss = 100 - Efficiency
Transmission time	The time required for transmission of a message depends on the size of the message and the bandwidth of the channel.	Transmission time=Message size / Bandwidth
Propagation Time	Propagation time measures the time required for a bit to travel from the source to the destination. The propagation time is calculated by dividing the distance by the propagation speed.	Propagation time = Distance /Propagation speed

Processing Delay	Time taken by the processor to process the data packet is called processing delay.	
Queuing Delay	Time spent by the data packet waiting in the queue before it is taken for execution is called queuing delay.	
Jitter	Jitter is defined as the variation in time delay for the data packets sent over a network. This variable represents an identified disruption in the normal sequencing of data packets. Jitter is related to latency, since the jitter manifests itself in increased or uneven latency between data packets, which can disrupt network performance and lead to packet loss and network congestion. Although some level of jitter is to be expected and can usually be tolerated, quantifying network jitter is an important aspect of comprehensive network	Latency=sum of all delays To measure Jitter, we take the difference between samples, then divide by the number of samples (minus 1).

Architecture diagram:





Analytical questions:

Post 10 questions and answers for various analytical questions regarding Banking network

1) **Question**: What is the role of encryption in securing banking networks?

   Answer: Encryption plays a crucial role in banking networks by encoding sensitive data during transmission, making it unreadable to unauthorized parties. This safeguards customer information, financial transactions, and communication within the network.

2) **Question:** How do banks use anomaly detection systems to identify potential security t hreats in their networks?

   Answer: Banks utilize anomaly detection systems that analyze network behavior to identify deviations from established patterns. This helps in real-time detection of unusual activities, such as unauthorized access or suspicious transactions, enabling prompt response to potential security threats.

3) **Question**: What measures do banks implement to protect against Distributed Denial of Service (DDoS) attacks on their networks?

   Answer: Banks employ DDoS mitigation strategies, including traffic filtering, load balancing, and content delivery networks. These measures help absorb and mitigate the impact of DDoS attacks, ensuring uninterrupted service for customers.

4) **Question**: How does the implementation of blockchain technology impact the security and transparency of banking networks?

   Answer: Blockchain enhances security and transparency in banking networks by providing a decentralized and tamper-resistant ledger. Smart contracts and cryptographic validation mechanisms contribute to secure, transparent, and efficient transaction processing.

5) **Question**: What role does artificial intelligence (AI) play in fraud detection within banking networks?

   Answer: AI is employed in banking networks for advanced fraud detection. Machine learning algorithms analyze vast amounts of data to identify patterns indicative of fraudulent activities, enabling banks to proactively prevent and mitigate potential risks.

6) **Question**: How do banks ensure compliance with data protection regulations when handling customer information in their networks?

   Answer: Banks implement robust data protection measures, including access controls, encryption, and regular audits, to comply with data protection regulations. Privacy impact

assessments and adherence to international standards contribute to maintaining the confidentiality and integrity of customer data.

7) **Question:** In what ways do banks employ biometric authentication to enhance network security?

Answer: Banks integrate biometric authentication methods, such as fingerprint and facial recognition, to enhance network security. Biometrics provide a more secure and user- friendly means of identity verification, reducing the risk of unauthorized access to banking systems.

8) **Question**: How do banks balance the need for accessibility and security in their mobile banking networks?

Answer: Banks implement multi-factor authentication, secure mobile apps, and continuous monitoring to balance accessibility and security in mobile banking networks. User education on secure practices and real-time transaction verification further contribute to a secure mobile banking experience.

9) **Question**: What role does network segmentation play in enhancing the security posture of banking networks?

Answer: Network segmentation is crucial in banking networks to isolate and compartmentalize different functions and user groups. This limits the impact of security breaches, preventing unauthorized access to sensitive data and critical systems.

10) **Question**: How do banks leverage threat intelligence to stay ahead of evolving cybersecurity threats in their networks?

Answer: Banks actively subscribe to threat intelligence services that provide real-time information on emerging cybersecurity threats. This enables proactive security measures, including timely updates to firewalls, intrusion detection systems, and other security protocols, to counter evolving threats in banking networks.

Department Name / Sub Network Name	**Student Roll No and Name**
FIRST FLOOR	CB.EN.U4CSE21322(JASWANTH G)
SECOND FLOOR	CB.EN.U4CSE21361(SAI SATYA)
THIRD FLOOR	CB.EN.U4CSE21329(HITEESH RAJU)
FOURTH FLOOR	CB.EN.U4CSE21328(ABHISHEK)

CISCO packet tracer Network design

FIRST FLOOR:

Department	Network Address	Subnet Mask	Host Address Range	Broadcast Address
Management	192.168.10.0	255.255.255.192/26	192.168.10.1 to 192.168.10.62	192.168.10.63
Research	192.168.10.64	255.255.255.192/26	192.168.10.65 to 192.168.10.126	192.168.10.127
Human Res	192.168.10.128	255.255.255.192/26	192.168.10.129 to 192.168.10.190	192.168.10.191

SECOND FLOOR:

Department	Network Address	Subnet Mask	Host Address Range	Broadcast Address
Marketing	192.168.10.192	255.255.255.192/26	192.168.10.193 to 192.168.10.254	192.168.10.255
Accounts	192.168.11.0	255.255.255.192/26	192.168.11.1 to 192.168.11.62	192.168.11.63
Finance	192.168.11.64	255.255.255.192/26	192.168.11.65 to 192.168.11.126	192.168.11.127

THIRD FLOOR:

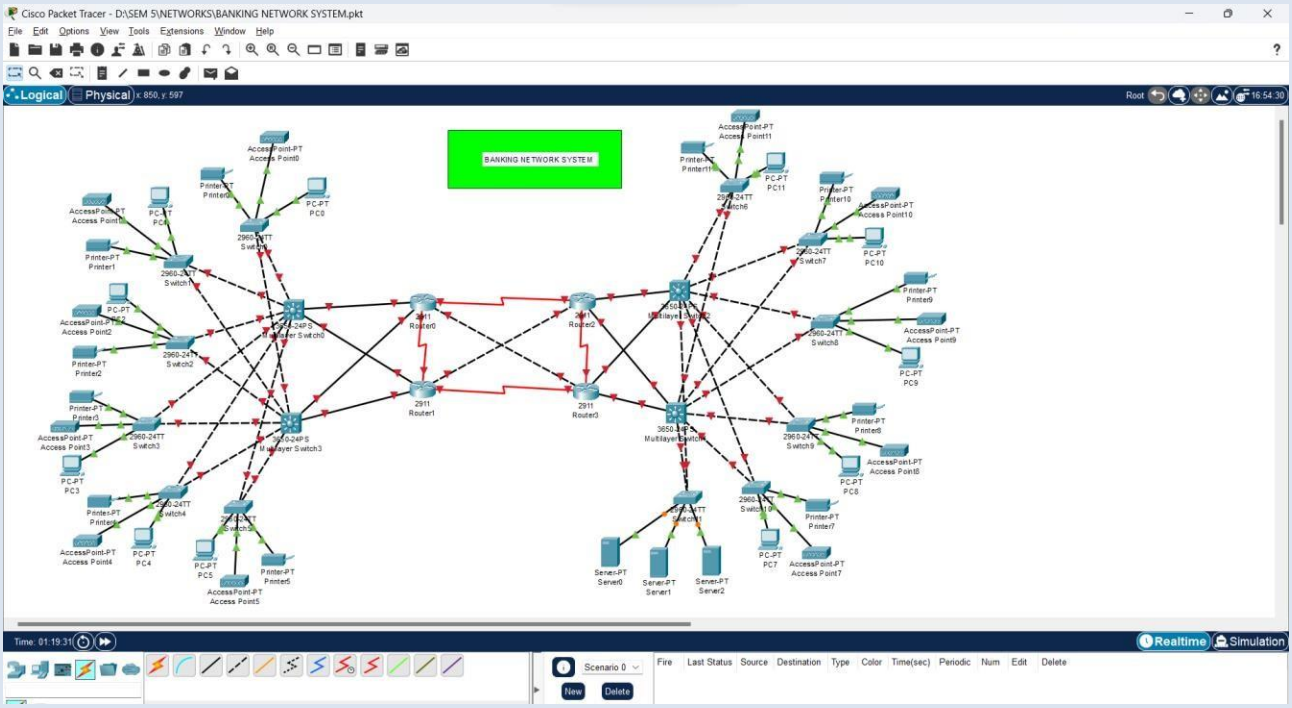
Department	Network Address	Subnet Mask	Host Address Range	Broadcast Address
Logistics	192.168.11.128	255.255.255.192/26	192.168.11.129 to 192.168.11.190	192.168.11.191
Customer	192.168.11.192	255.255.255.192/26	192.168.11.193 to 192.168.11.254	192.168.11.255
Guest	192.168.12.0	255.255.255.192/26	192.168.12.1 to 192.168.12.62	192.168.12.63

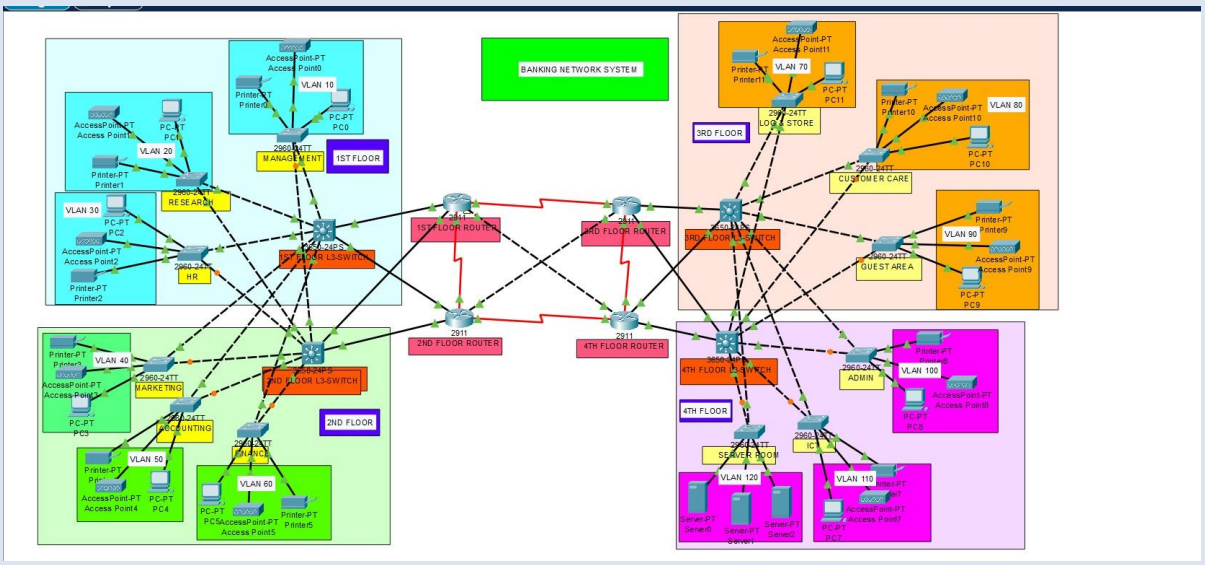
FOURTH FLOOR:

Department	Network Address	Subnet Mask	Host Address Range	Broadcast Address
Admin	192.168.12.64	255.255.255.192/26	192.168.12.65 to 192.168.12.126	192.168.12.127
ICT	192.168.12.128	255.255.255.192/26	192.168.12.129 to 192.168.12.190	192.168.12.191
Server Room	192.168.12.192	255.255.255.192/26	192.168.12.193 to 192.168.12.254	192.168.12.255

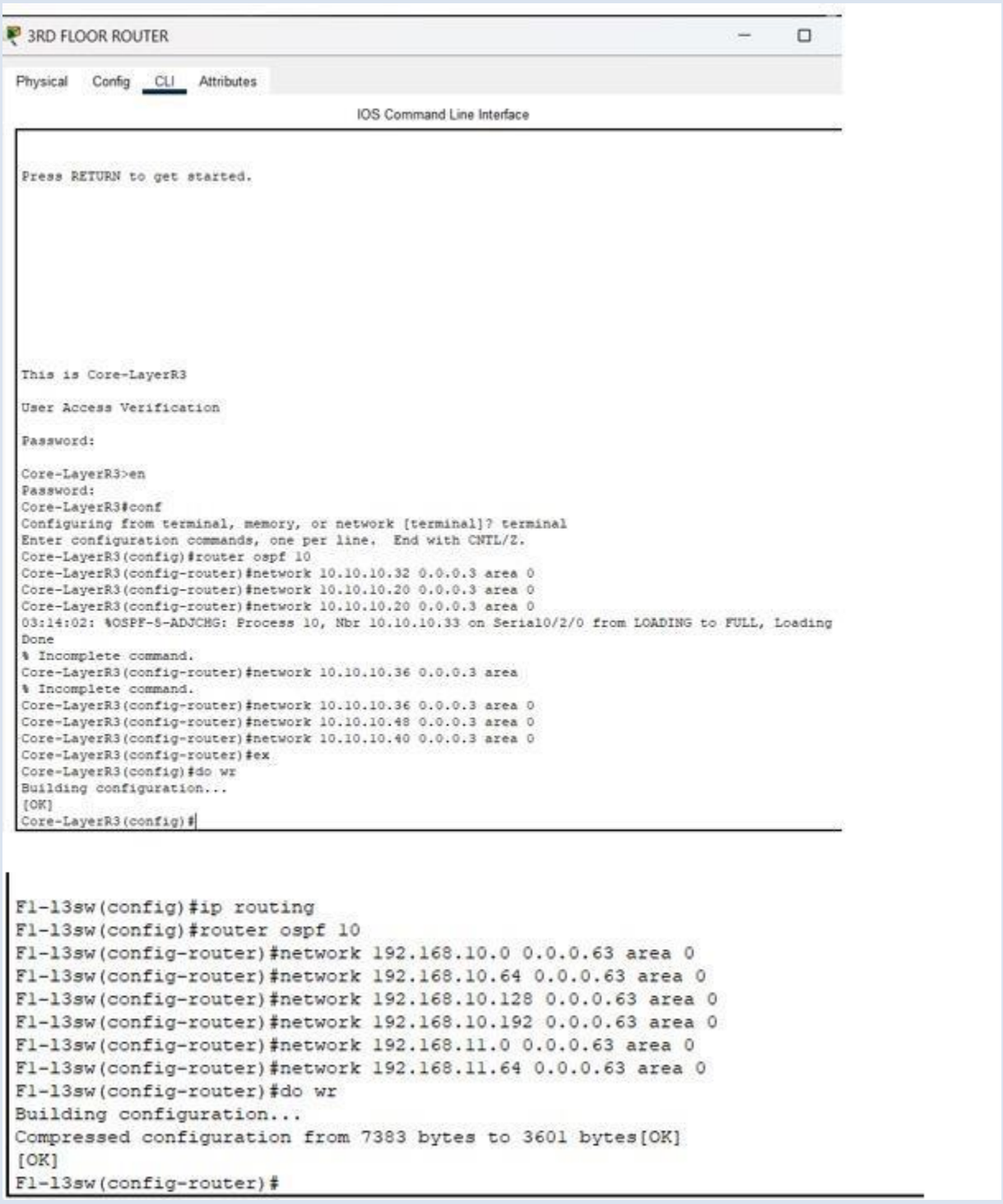
DEVICES USED:

1. 4 Routers – 2911
2. 4 Switches – 3650
3. 12 Departments – 3 per each floor





Routing Algorithm




```
Fl-l3sw(config)#ip routing
Fl-l3sw(config)#router ospf 10
Fl-l3sw(config-router)#network 192.168.10.0 0.0.0.63 area 0
Fl-l3sw(config-router)#network 192.168.10.64 0.0.0.63 area 0
Fl-l3sw(config-router)#network 192.168.10.128 0.0.0.63 area 0
Fl-l3sw(config-router)#network 192.168.10.192 0.0.0.63 area 0
Fl-l3sw(config-router)#network 192.168.11.0 0.0.0.63 area 0
Fl-l3sw(config-router)#network 192.168.11.64 0.0.0.63 area 0
Fl-l3sw(config-router)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
Fl-l3sw(config-router)#
```