SAVEETHA SCHOOL OF ENGINEERING

Engineer to Excel

CAPSTONE PROJECT

Designing and Implementing a Secure and Scalable Network Architecture for Telecommunication Companies

NAME: Sayed Fazal

REGISTER NUMBER: 192311291

COURSE CODE: CSA0747

COURSE NAME: Computer Network for IOT

INTRODUCTION:

In today's digital era, telecommunication companies are at the forefront of enabling global communication. However, this critical role also makes them prime targets for cyber threats. Ensuring the security, scalability, and performance of telecommunication network systems is crucial for maintaining confidentiality, integrity, and availability. This project aims to develop a robust network architecture tailored for a telecommunication company, focusing on creating a resilient infrastructure capable of withstanding various cyber threats while ensuring seamless service delivery.

Objective:

- Develop a comprehensive network design that incorporates industry best practices to ensure security against cyber threats.
- Integrate encryption, access control, and monitoring mechanisms to safeguard the network infrastructure.
- Design the network to handle increasing loads while maintaining high performance.
- Test the implemented network system for vulnerabilities and performance issues, and provide recommendations for optimization.

LITERATURE REVIEW

Telecommunication networks are essential for transmitting sensitive and critical information. Studies emphasize the growing need for advanced security measures in protecting these networks from emerging cyber threats. Industry standards and best practices in network design are pivotal in ensuring security and efficiency. Effective monitoring and incident response are vital for identifying and mitigating security threats.

METHODOLOGY

Software:

- Cisco Packet Tracer

Network Design:

Network consist of

- 21 servers
- 10 switches
- 9 routers
- 12 PCs
- 14 laptops
- 7 smartphones
- 4 wireless controllers

All routers were connected to one another, and each two routers connected two switches, with the third router connecting to a single switch. The first four switches connected two PCs, and the third switch connected two servers.

IP Address Allocation:
Step 1: Switch 1 Configuration
Devices: Two PCs and one router
IP Addresses:
Router1 IP Address: 192.168.10.1
PC0 IP Address: 192.168.10.2
PC1 IP Address: 192.168.10.3

Step 2: Switch 2 Configuration
Devices: Two PCs and one router
IP Addresses:
Router1 IP Address: 192.168.20.1
PC2 IP Address: 192.168.20.2
PC3 IP Address: 192.168.20.3

Step 3: Switch 3 Configuration
Devices: Two PCs and one router
IP Addresses:
Router2 IP Address: 192.168.30.1
PC4 IP Address: 192.168.30.2
PC5 IP Address: 192.168.30.3

Step 4: Switch 4 Configuration
Devices: Two PCs and one router
IP Addresses:
Router2 IP Address: 192.168.40.1
PC6 IP Address: 192.168.40.2
PC7 IP Address: 192.168.40.3

Step 5: Switch 5 Configuration
Devices: Two servers and one router
IP Addresses:
Router3 IP Address: 192.168.50.1
Server1 IP Address: 192.168.50.2
Server2 IP Address: 192.168.50.3

Step 6: Interconnecting Routers
Router Connections:
Router1 IP Address (out): 10.0.0.1
Router2 IP Address (in): 10.0.0.2
Router2 IP Address (out): 20.0.0.1
Router3 IP Address (in): 20.0.0.2

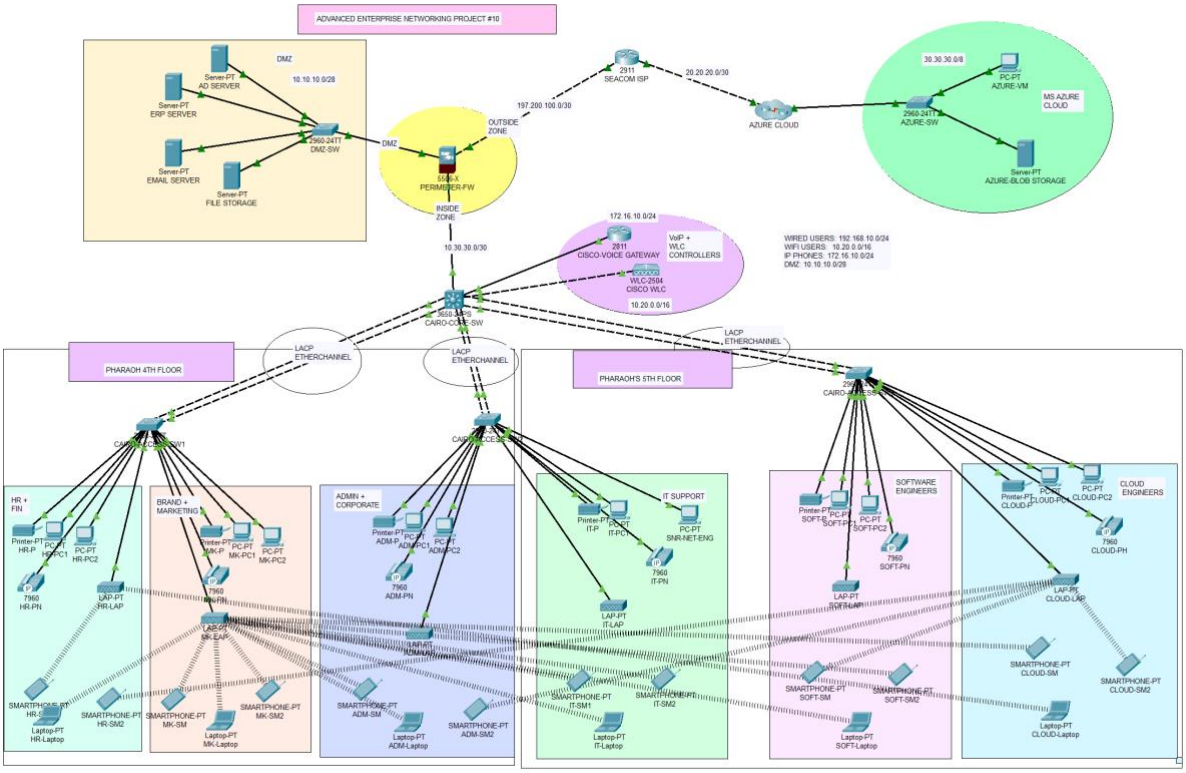
Step 7: Routing Information Protocol (RIP) Configuration.

Protocol: - HTTP

- HTTP is the communication protocol used on the World Wide Web.
- It specifies how communications (requests and responses) are prepared and sent between clients (such web browsers) and servers.
- Stateless protocol: Each request-response cycle is distinct; the server does not maintain information from prior encounters**.**

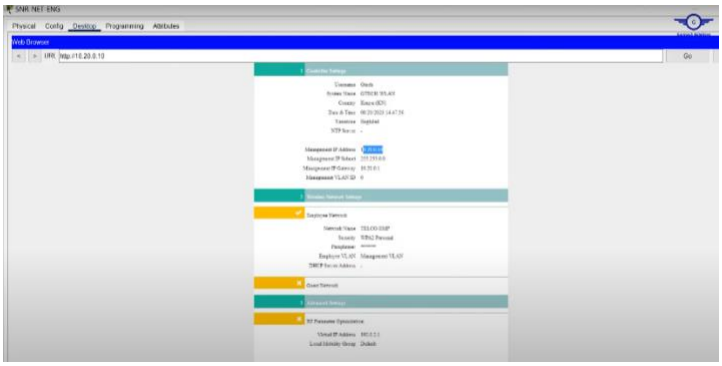
RESULT:

Network Design:



- open pc -> desktop -> web browser

- enter web URL -> according web site pop ups



CONCLUSION:

Cisco Packet Tracer is a network simulation tool that is not intended to directly deploy online services, such as genuine web servers. However, it can be an effective tool for imitating and comprehending how web services work in a networked setting. Designing and implementing a secure and scalable network architecture for telecommunication companies is a complex but essential endeavour for ensuring robust and reliable communication services. Through our project, we have explored various aspects of network architecture, from fundamental principles to advanced security measures and scalability strategies.

Here's a summary of what you can achieve with Cisco Packet Tracer regarding web services:

1. **Security:** Implementing a multi-layered security approach, including firewalls, intrusion detection/prevention systems (IDS/IPS), and encryption, is crucial for safeguarding sensitive data and maintaining the integrity of communication networks. Regular security assessments and updates are necessary to address emerging threats and vulnerabilities.
2. **Scalability:** Designing for scalability involves choosing modular and flexible solutions that can adapt to growing demands. Techniques such as network segmentation, load balancing, and cloud-based resources help manage increased traffic and support future growth without compromising performance.
3. **Redundancy and Reliability:** Incorporating redundancy through failover mechanisms and diverse routing paths ensures high availability and minimizes downtime. Our design integrates multiple data paths and backup systems to maintain continuous service even in the event of component failures.
4. **Performance Optimization:** Leveraging technologies such as Quality of Service (QoS) and Content Delivery Networks (CDNs) enhances network performance by prioritizing critical traffic and optimizing content distribution.
5. **Compliance and Best Practices:** Adhering to industry standards and regulatory requirements is essential for maintaining trust and ensuring that our network architecture meets legal and operational obligations.