Design, Implementation, and Testing of a Segmented Network Infrastructure for a Multifloor Organization

Samiha Nazrul
Information Systems & Computer Security
(Data Science)
Tuskegee, Alabama, United States
snazrul5756@tuskegee.edu

Aditi Saha
Information Systems & Computer Security
(Data Science)
Tuskegee, Alabama, United States
asaha5032@tuskegee.edu

***Abstract*—This paper presents the design, implementation, and testing of a segmented network infrastructure tailored for a multifloor organization. The organization's three-floor building is equipped with distinct departments, each requiring isolated network environments for optimal functionality. Through careful subnetting and VLAN configuration, the network achieves efficient departmental segmentation. The routers interconnecting the floors employ the OSPF routing protocol, facilitating seamless communication across the organization. Rigorous testing confirms the successful sharing of resources, including printers, internal web services, and SSH access. The implementation includes essential services such as DHCP, DNS, web, email, and file servers, ensuring a robust and fully functional network. The results indicate successful achievement of network objectives, meeting the organization's diverse requirements. This paper provides valuable insights into the design principles and testing methodologies employed, offering a comprehensive overview of the implemented network infrastructure.**

Keywords- Subnet; VLAN; DHCP; Server; IP; Router

I. INTRODUCTION

In the ever-evolving landscape of organizational networks, this paper explores the tailored design, implementation, and testing of a segmented infrastructure for a three-floor organization. The organization's diverse departments necessitated a network configuration that ensures both isolation and efficient communication. Achieving this balance involved meticulous subnetting, VLAN configuration, and the deployment of OSPF routing between floors. Essential services, including DHCP, DNS, web, email, and file servers, were implemented within the IT department. This paper outlines the specifics of design choices, implementation strategies, and rigorous testing, offering insights for organizations seeking a scalable and secure network blueprint.

II. NETWORK DESIGN AND IMPLEMENTATION

A. Subnetting and VLAN Configuration

The foundation of the network design involved the systematic subdivision of the given IP address space (192.168.1.0/24) to accommodate the unique requirements of each department. Subnetting ensured efficient utilization of IP addresses and facilitated the isolation of departmental networks. VLANs were configured on network switches to segment traffic and enable distinct broadcast domains for each department. The following VLANs were established:

VLAN 10: IT Department (192.168.1.0/24)

- Subnet: 192.168.1.0/24
- Gateway: 192.168.1.1
- Usable IP Range: 192.168.1.2 to 192.168.1.254
- Broadcast Address: 192.168.1.255

VLAN 20: Admin Department (192.168.2.0/24)

- Subnet: 192.168.2.0/24
- Gateway: 192.168.2.1
- Usable IP Range: 192.168.2.2 to 192.168.2.254
- Broadcast Address: 192.168.2.255

VLAN 30: Customer Care Department (192.168.3.0/24)

- Subnet: 192.168.3.0/24
- Gateway: 192.168.3.1
- Usable IP Range: 192.168.3.2 to 192.168.3.254
- Broadcast Address: 192.168.3.255

VLAN 40: Finance Department (192.168.4.0/24)

- Subnet: 192.168.4.0/24
- Gateway: 192.168.4.1
- Usable IP Range: 192.168.4.2 to 192.168.4.254
- Broadcast Address: 192.168.4.255

VLAN 50: Sales Department (192.168.5.0/24)

- Subnet: 192.168.5.0/24
- Gateway: 192.168.5.1
- Usable IP Range: 192.168.5.2 to 192.168.5.254
- Broadcast Address: 192.168.5.255

VLAN 60: HR Department (192.168.6.0/24)

- Subnet: 192.168.6.0/24
- Gateway: 192.168.6.1
- Usable IP Range: 192.168.6.2 to 192.168.6.254
- Broadcast Address: 192.168.6.255

VLAN 70: Reception Department (192.168.7.0/24)

- Subnet: 192.168.7.0/24
- Gateway: 192.168.7.1
- Usable IP Range: 192.168.7.2 to 192.168.7.254
- Broadcast Address: 192.168.7.255

VLAN 80: Store Department (192.168.8.0/24)

- Subnet: 192.168.8.0/24
- Gateway: 192.168.8.1
- Usable IP Range: 192.168.8.2 to 192.168.8.254

- Broadcast Address: 192.168.8.255

B. *Router Configuration*

To facilitate communication between departments, three routers on each floor were placed in mesh-setting. The routers were configured with OSPF (Open Shortest Path First) as the routing protocol. Interconnecting subnets were assigned as follows:

Router 1 ↔ Router 2: 10.10.10.8/30

Router 2 ↔ Router 3: 10.10.10.0/30

Router 3 ↔ Router 1: 10.10.10.4/30

This setup enabled dynamic routing, ensuring efficient and automatic path selection.

C. *Switch and Access Point Configuration*

Each floor is equipped with a dedicated switch to connect the devices within that floor. A total of three switches are employed, ensuring efficient connectivity within each department. Access points are strategically placed to provide wireless network coverage for each department. Laptops within departments connect to the respective access points to access the wireless network.

D. *Services Configuration*

Within the IT department, critical services were configured to meet the organization's operational needs:

- DHCP: Automatically assigned IP addresses to devices within each VLAN.
- DNS: Resolved domain names and enabled external access to web, SSH, and email services.
- Web Server: Hosted a default web page accessible within the organization.
- Email Server: Facilitated internal email communication.
- File Server: Provided storage for users within the organization.

The configurations were meticulously implemented to ensure the seamless operation of these services.

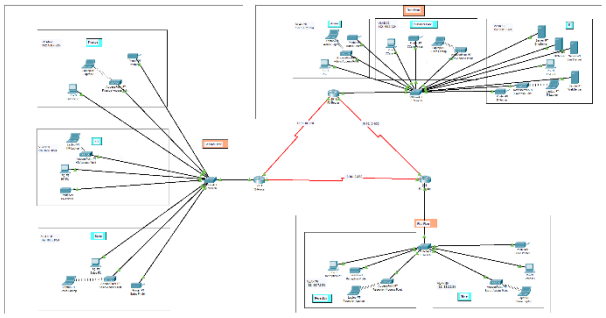
E. *Printer Placement*

Printers are strategically placed within each department for easy accessibility by users. Static IP addresses are assigned to printers to ensure consistent availability.

This comprehensive network design and implementation aimed to address the unique requirements of each department while fostering interdepartmental communication and resource sharing. The subsequent section details the rigorous testing conducted to validate the efficacy of the implemented network.

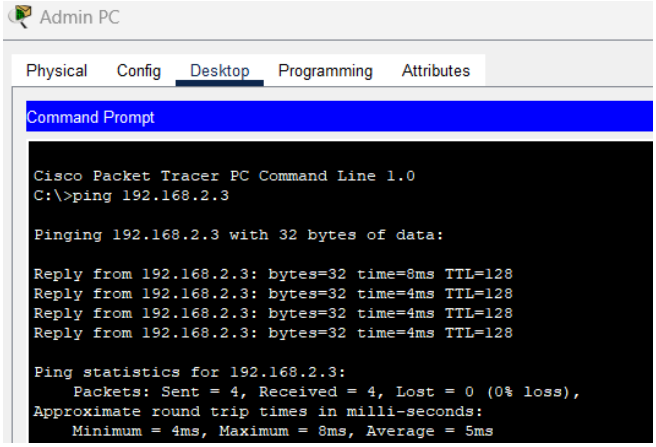
III. Testing and Results

A thorough testing regime was executed to validate the efficacy of the implemented network infrastructure. The following sections detail the outcomes of rigorous assessments conducted across key network functionalities. From printer sharing to secure remote access, each aspect underwent scrutiny to ensure seamless interdepartmental communication, resource accessibility, and the overall success of the network design. The results serve as a testament to the careful planning and execution of the network configuration, reflecting its ability to meet the diverse requirements of the multifloored organization. The total project outline has been shown below as well.



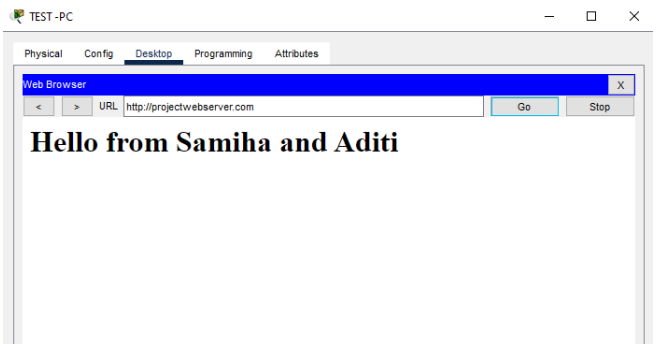
A. *Printer Sharing*

Printer sharing functionality was thoroughly tested to confirm seamless access within the local area network (LAN). Users from each department successfully connected to and printed documents on their respective printers. This result underscores the effective VLAN segmentation and inter-VLAN communication facilitated by the router configurations. Below is a screenshot of ping command from Admin PC to Admin Printer:



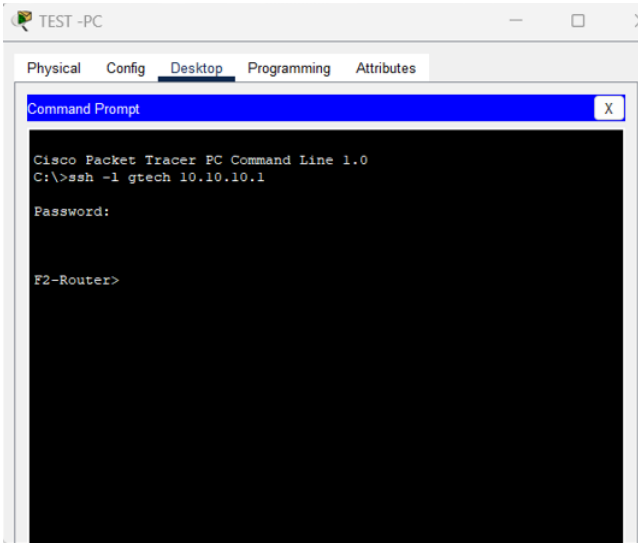
B. *Webserver/Website Access*

The accessibility of the webserver and website was verified by users across different departments. Internal testing confirmed that any PC within the organization could successfully reach the webserver, demonstrating the effectiveness of the routing protocols and interdepartmental connectivity. Below is a screenshot of accessing projectwebserver.com from browser of TEST-PC:



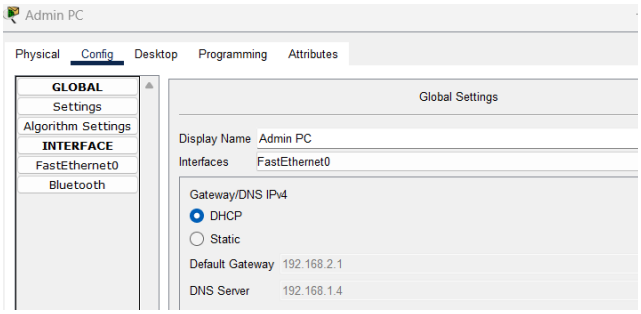
C. SSH Access

Secure Shell (SSH) access to the 'Test' PC in the IT department was tested internally. The 'Test' PC successfully established a remote SSH connection to the F2-Router, demonstrating the secure configuration of SSH and the effective implementation of network security measures. Here, username and password used both are gtech.



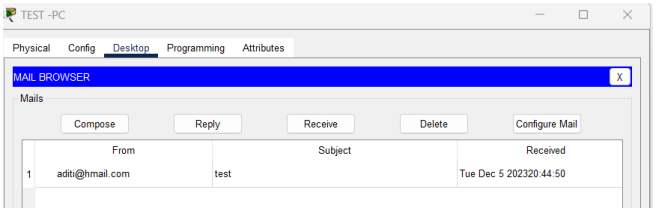
D. DHCP Functionality

The DHCP service was rigorously tested to ensure that devices across departments could dynamically obtain IP addresses. Devices successfully received IP addresses automatically, confirming the proper functioning of the DHCP server and the integrity of the subnetting and VLAN configurations.



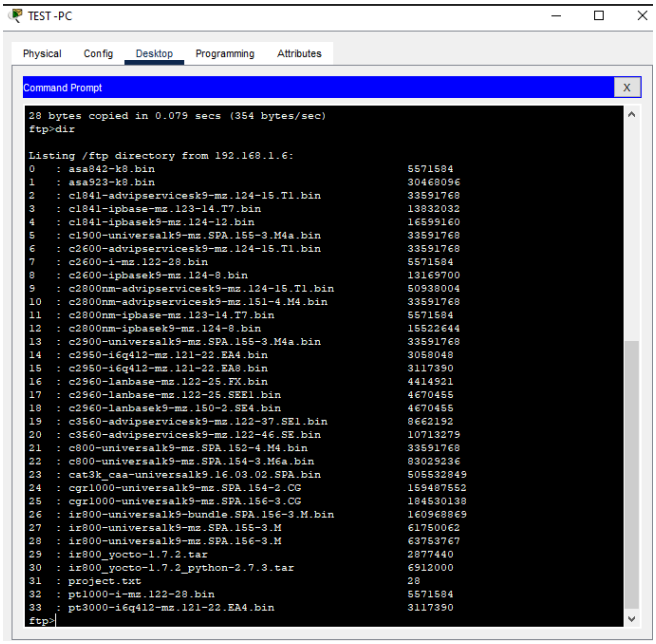
E. Email Functionality

Testing internal email communication validated the proper operation of the email server. Users within the organization could send and receive emails, ensuring effective collaboration and communication across departments.



F. File Server Operation

Testing the File Transfer Protocol (FTP) functionality involved utilizing a PC to access the FTP server securely. Upon successful login with a designated username and password, a file named 'project.txt' was uploaded to the FTP server. Verification was performed by executing the 'dir' command, confirming the presence of the uploaded file on the server. This validated the reliable and secure file exchange capabilities provided by the FTP server, contributing to streamlined collaboration and resource sharing within the organization.



IV. Discussion

The successful implementation of the network infrastructure has yielded positive outcomes across various aspects. Subnetting and VLAN configuration effectively segmented the network, ensuring departmental isolation while facilitating seamless communication. Router configuration, coupled with OSPF routing, provided dynamic and optimal paths for interdepartmental connectivity. The deployment of critical services within the IT department, including DHCP, DNS, web, email, and file servers, establishes a centralized hub for efficient network management. Rigorous testing confirmed the reliability of printer sharing, webserver accessibility, SSH access, DHCP functionality, email

communication, and file server operation. The modular design allows for adaptability to future organizational changes and expansions. Additionally, the security measures, including secure SSH access and controlled external DNS, contribute to a robust and resilient network. Overall, the implemented network configuration successfully meets the organization's objectives and sets the groundwork for scalability and future advancements.

V. FUTURE WORK

While the current network design successfully meets the outlined requirements, there are avenues for future enhancements and expansions. Notably, the incorporation of Network Address Translation (NAT) and enabling outside access to internal services could fortify the organization's network security and facilitate external collaborations. Future endeavors may focus on implementing these features, further enhancing the network's capabilities and ensuring its alignment with evolving technological needs and security standards.

ACKNOWLEDGMENT

We would like to express our sincere gratitude to Dr. Mohammad Arafatur Rahman for his invaluable guidance and support throughout the duration of this project. His expertise, encouragement, and insightful feedback have played a pivotal role in shaping our understanding of network design and implementation. We appreciate his dedication to fostering a collaborative learning environment and his commitment to our academic and professional development. His mentorship has been instrumental in the successful completion of this project.

REFERENCES

[1] "CompTIA Network+ Study Guide: Exam N10-007" by Todd Lammle

[2] "Computer Networking: Principles, Protocols and Practice" by Olivier Bonaventure.