**DATA COMMUNICATION AND COMPUTER NETWORKS**

**REPORT**

**MUHAMMAD TALHA ALI BUTT**

2025

Report

# Table of Contents

1. Introduction

2. Network Access Control Policies

- 2.1 IT Department Privileged Access

- 2.2 Restricted Access for Other Departments

3. Core Network Traffic Filtering

- 3.1 ICMP, DNS, DHCP, HTTP Allowed

- 3.2 Traffic Filtering Policies

4. IT Department Switch Security

- 4.1 Port Security Implementation

- 4.2 Violation Response Strategy

5. Spanning Tree Protocol in SMT Network

- 5.1 STP Configuration and Purpose

- 5.2 Observations

6. VLAN Configuration in SMT Department (Area 1)

- 6.1 VLAN for Postpaid Management

- 6.2 VLAN for Prepaid Management

7. Inter-Department Access Restrictions

- 7.1 OMD to Postpaid SMT Restrictions

- 7.2 OMD to NOC Web Server Restrictions

- 7.3 PB to Prepaid SMT Restrictions

8. DHCP Configuration

- 8.1 Centralized DHCP Server in NOC

- 8.2 DHCP Relay Configuration

9. DNS Configuration

- 9.1 DNS Server Placement

- 9.2 DNS Accessibility and Scope

10. OSPF Configuration and Optimization

- 10.1 Multi-area OSPF Design

- 10.2 Route Summarization Strategy

11. IP Address Allocation Strategy

- 11.1 Subnetting with Least Wastage

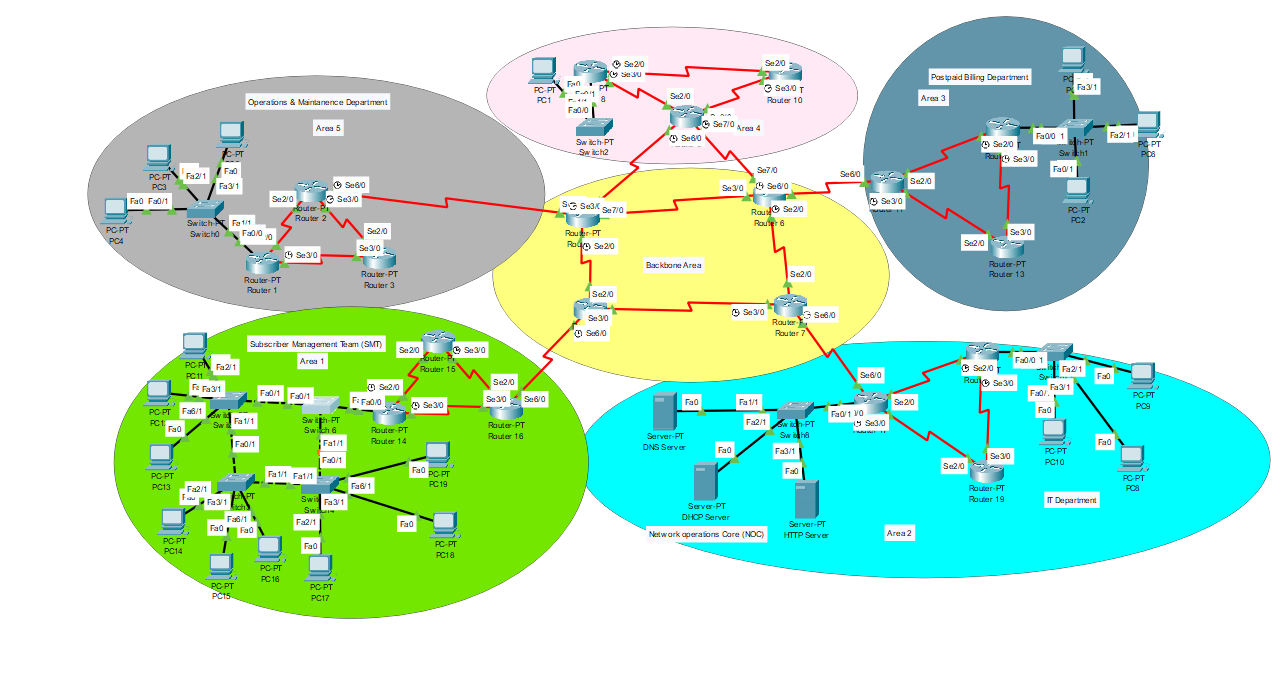
- 11.2 Address Plan Overview

12. Conclusion

## 1. Introduction

**This report presents a comprehensive analysis of the sample network topology and operational requirements provided by Mobilink Pakistan. As a Network Solutions Architect candidate, my primary objective is to deliver a strategic, scalable, and secure network design that aligns with the organization's current and future goals. The approach documented herein emphasizes best practices in network segmentation, security enforcement, traffic optimization, and dynamic routing using OSPF.**

**Through a methodical breakdown of each requirement, I have proposed practical solutions involving VLAN configuration, ACL implementation, DHCP and DNS setup, STP functionality, and route summarization. The proposed architecture is designed to support seamless inter-departmental communication where necessary, while enforcing strict access controls to ensure data integrity, confidentiality, and compliance with internal IT policies. Additionally, the design takes into account efficient IP address allocation using VLSM to minimize wastage and enhance address management. This report aims to serve as a blueprint for deploying a resilient, high-performance enterprise network infrastructure tailored to Mobilink Pakistan’s operational needs.**

. ****

## 2.1 IT Department Privileged Access

Routers are configured with ACLs that allow full access from IT department subnets to all other departments. This includes enabling protocols like ICMP and Telnet for monitoring and remote management. The configuration ensures IT personnel can effectively manage and troubleshoot network devices.

## 

## 2.2 Restricted Access for Other Departments

## ACLs will deny all access from non-IT departments to the IT department, except for ICMP traffic. This ensures limited connectivity for basic network diagnostics while maintaining security. Ingress and egress filtering will be implemented to control and monitor traffic flow effectively.

## 3.1 Permitted Protocols

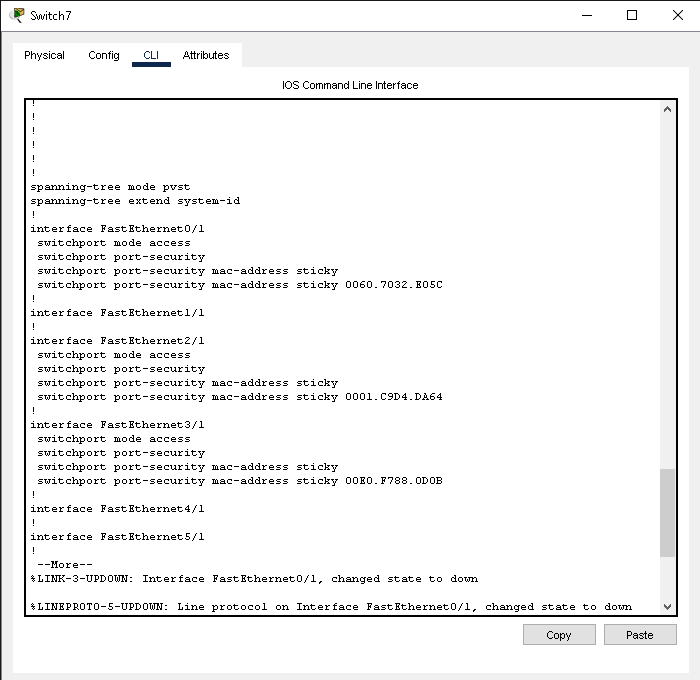
## ACLs at the Network Operations Core are configured to permit only essential traffic types. Allowed protocols include ICMP, DNS (UDP port 53), DHCP (UDP ports 67 and 68), and HTTP (TCP port 80). This ensures secure and controlled access while supporting basic network functionality.

## 3.2 Blocked Traffic

## All other protocols will be explicitly denied at the edge of the Network Operations Center (NOC). This ensures that only approved traffic types are allowed into the core network. It enhances security by blocking unauthorized or potentially harmful communications.

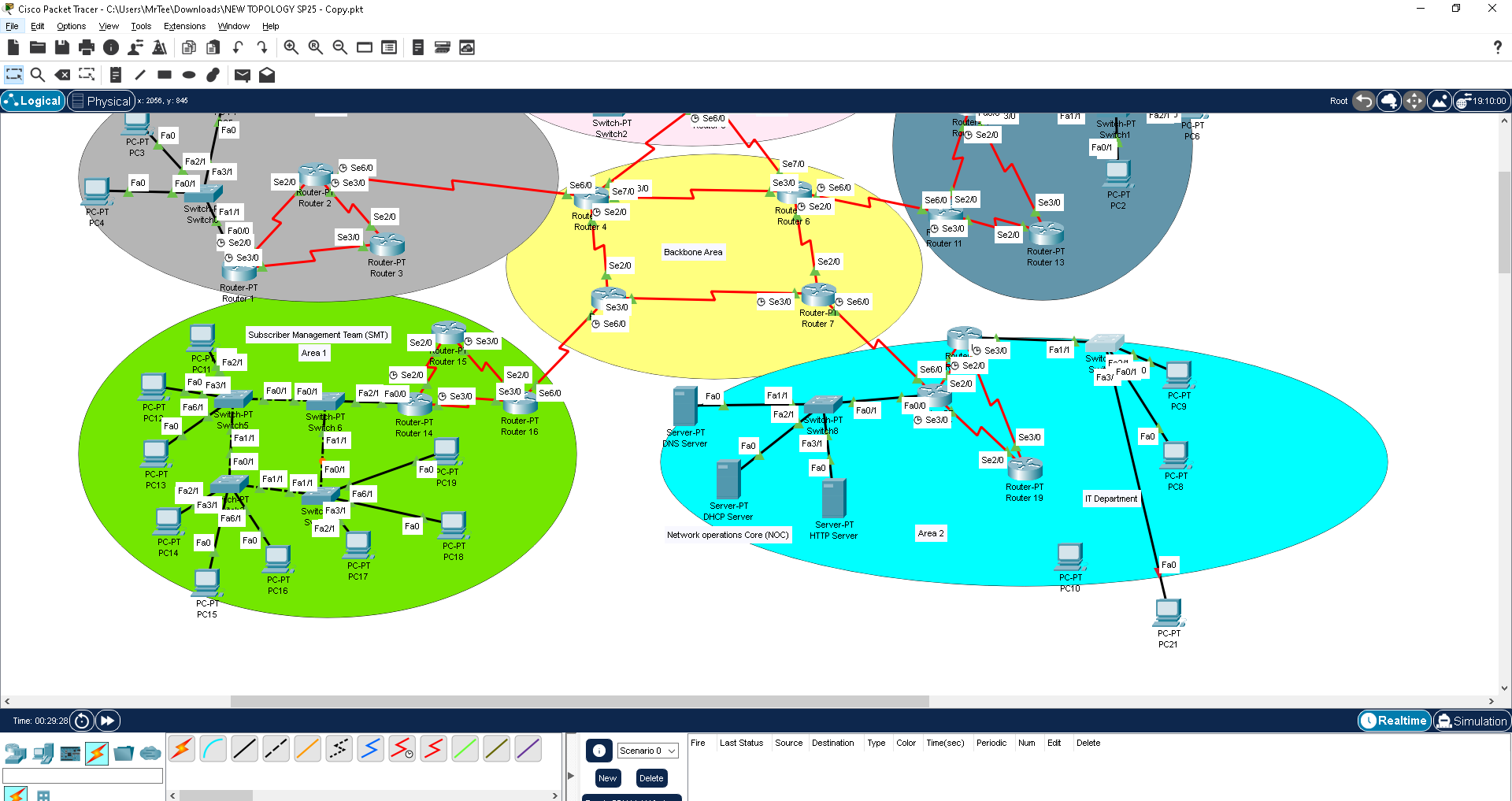
## 4.1 Port Security Configuration

Ports are secured by binding them to specific MAC addresses to prevent unauthorized device access. The switchport port-security command is enabled on each interface to enforce this control. If a violation occurs, the configured action is to immediately shut down the port.



## 4.2 Intrusion Response

If an unknown MAC address is detected on a secured port, the switch immediately shuts down the port. A log entry is generated to record the security violation for auditing and troubleshooting.



## 5.1 STP Configuration

## Spanning Tree Protocol (STP) is enabled on all switches to prevent Layer 2 loops and ensure network stability. The root bridge is manually configured to maintain control over the network topology.

## 5.2 Observations

No Layer 2 loops have been observed in the network, indicating stable STP operation. Ports are correctly transitioning between blocking and forwarding states as per STP logic. This confirms that the topology is optimized and loop-free.

A screenshot of a computer

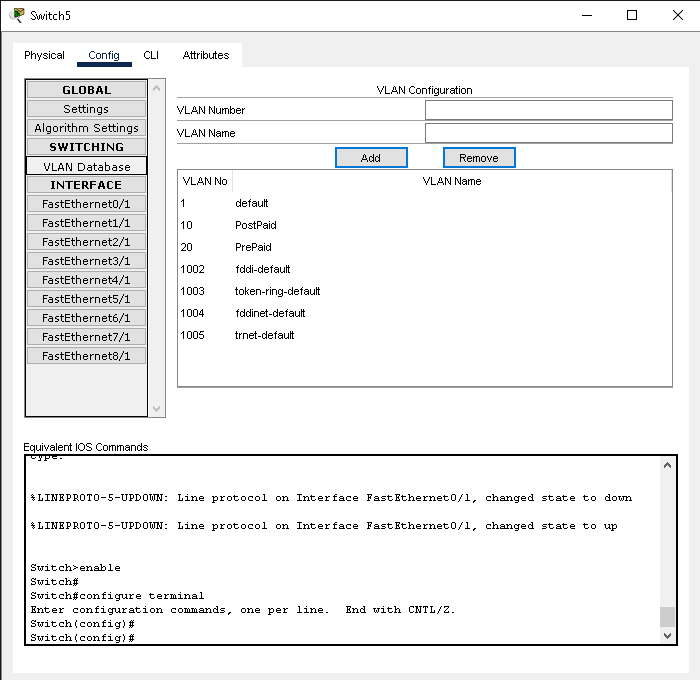
AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

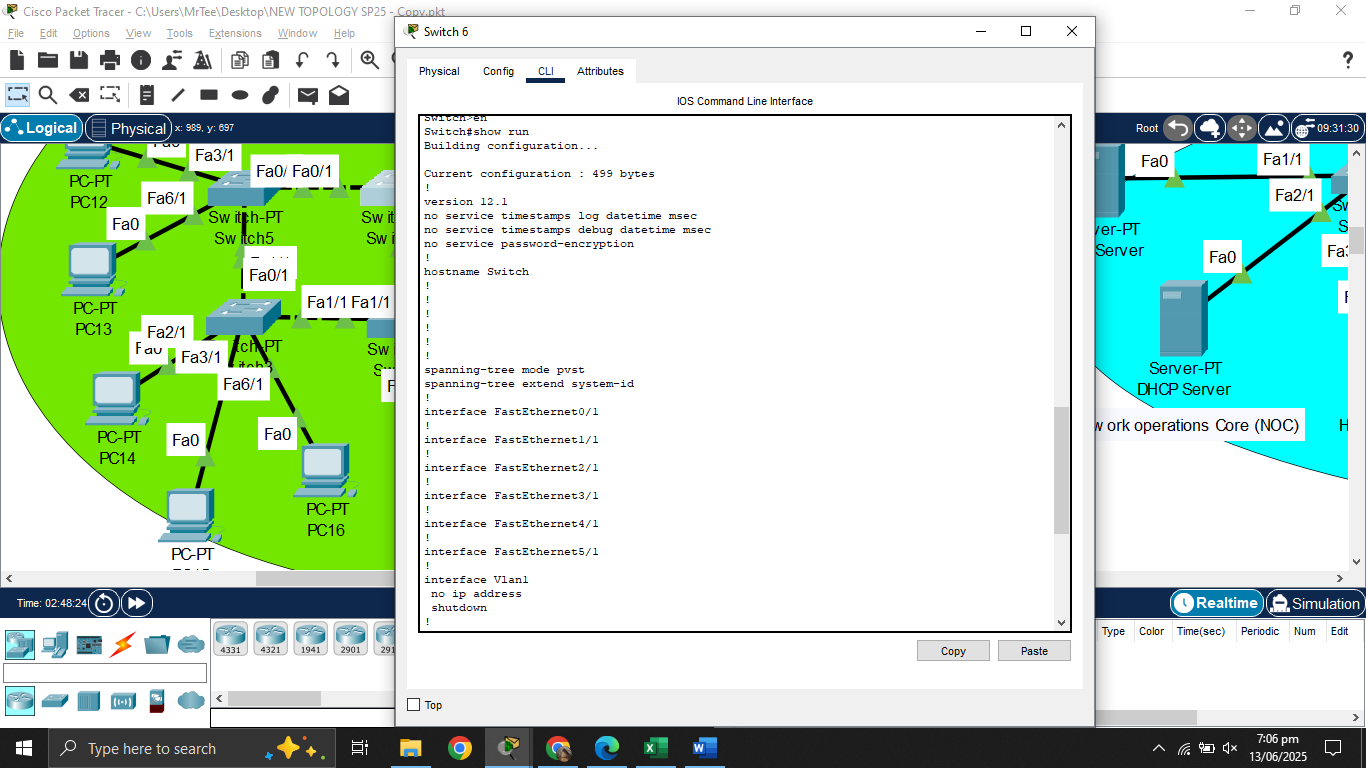
## 6.1 VLAN Assignments

VLAN 10 is assigned to the Postpaid Management team, supporting 5 users.  
VLAN 20 is designated for the Prepaid Management team, with 4 users connected.



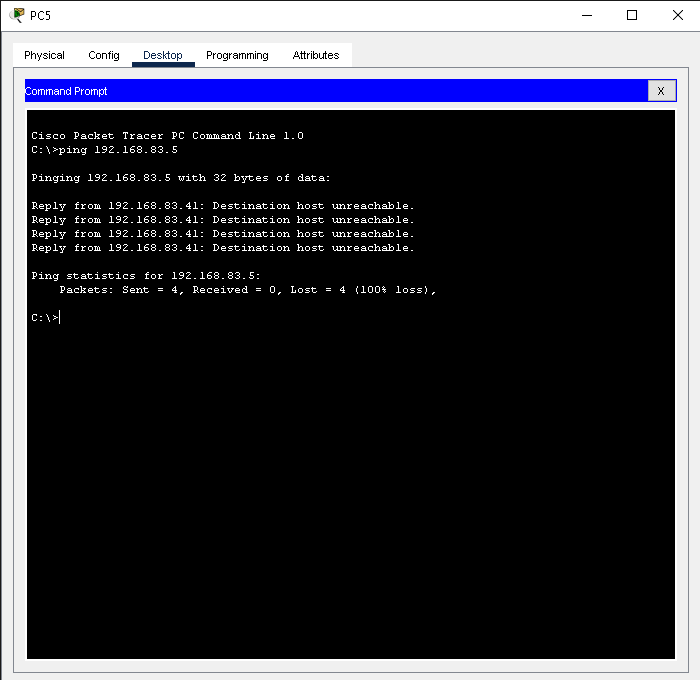
## 6.2 Inter-VLAN Routing

Inter-VLAN communication is controlled using a Layer 3 switch or a router-on-a-stick setup. Access Control Lists (ACLs) are implemented to prevent unauthorized cross-access between VLANs. This ensures secure communication while maintaining logical separation of network segments.



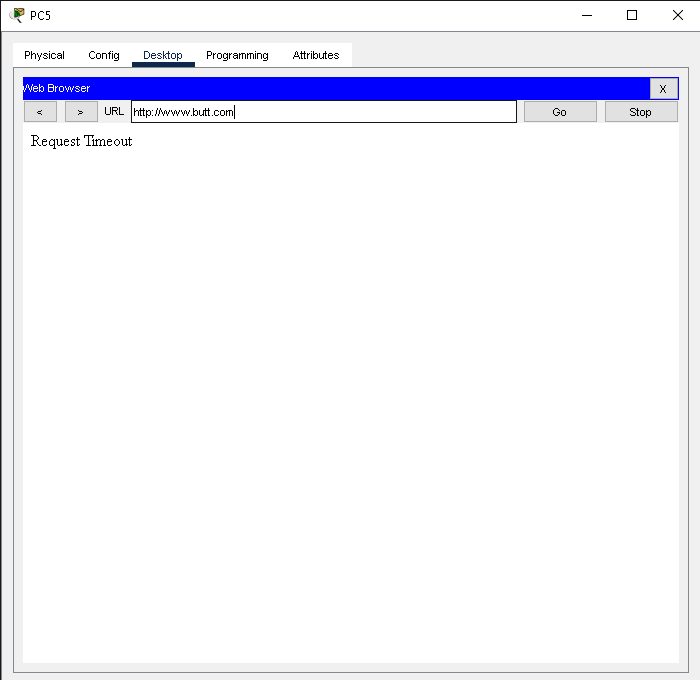
## 7.1 OMD to Postpaid SMT Restriction

Deny ACLs are configured between the OMD subnet and VLAN 10 to restrict communication. This prevents users in the OMD subnet from accessing devices or resources within VLAN 10.



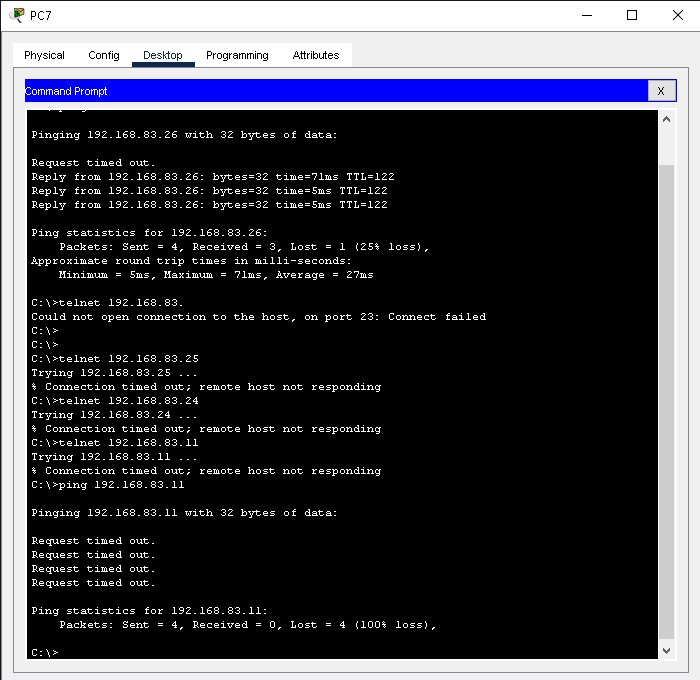
## 7.2 OMD to NOC Web Server

An ACL is configured to block TCP port 80 traffic from the OMD IP range to the NOC web server. This prevents HTTP access from OMD users, enhancing security and restricting unauthorized web access. Only approved sources are permitted to reach the NOC's web-based services.



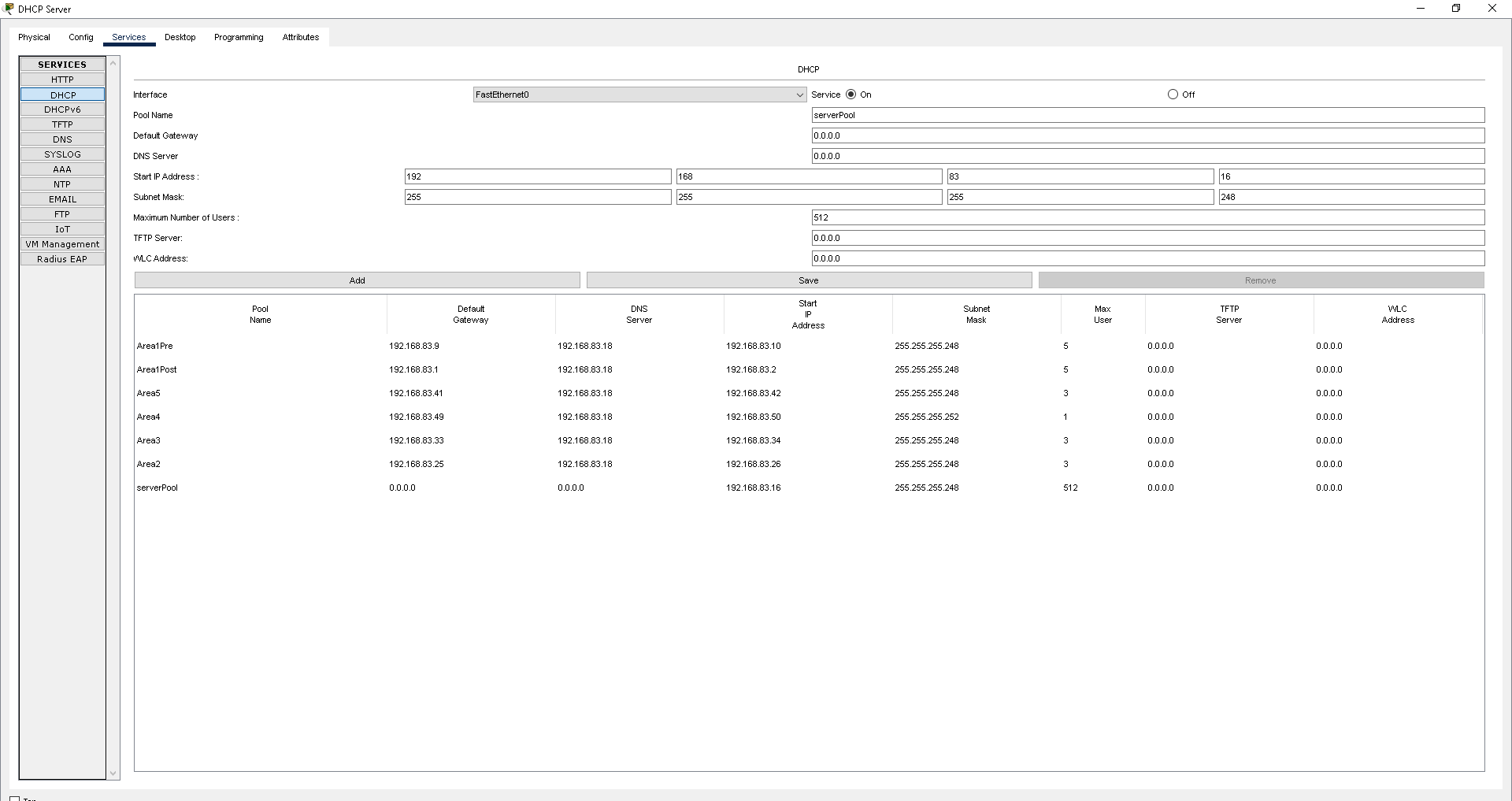
## 7.3 PB to Prepaid SMT Restriction

An ACL is implemented to deny any traffic from PB to VLAN 20 (Prepaid SMT). This ensures isolation between the two departments, preventing unauthorized access or data exchange. The rule enforces security policies and maintains VLAN-based segmentation.



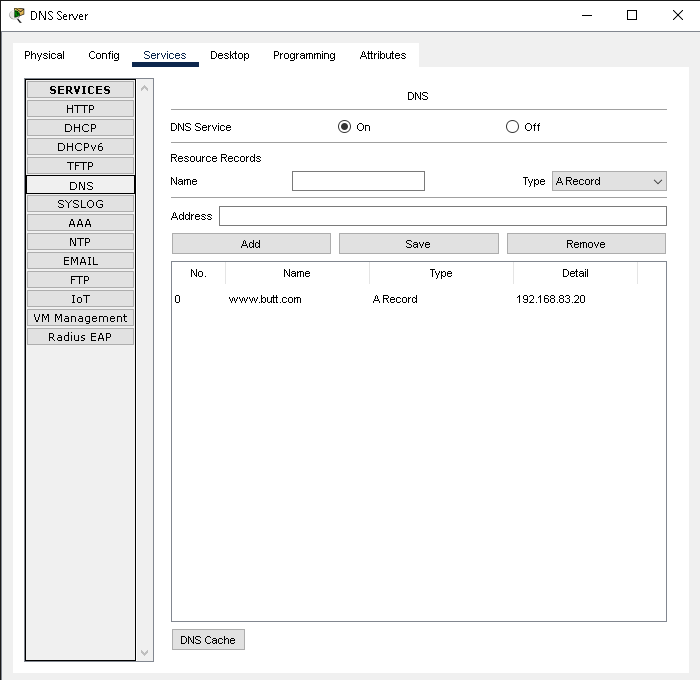
## 8.1 Centralized DHCP

A centralized DHCP server will be deployed in the Network Operations Center (NOC), configured with well-defined scope definitions for each departmental subnet. These scopes will include the appropriate IP address ranges, subnet masks, default gateways, DNS server addresses, and lease durations tailored to the needs of each network segment. By centralizing DHCP services, we ensure streamlined IP address management, simplified configuration, and consistent network policy enforcement across all departments. The design will also incorporate DHCP relay agents (using the ip helper-address command) on intermediate routers to facilitate IP address allocation to remote subnets without requiring additional DHCP servers.



## 9.1 DNS Server

## A dedicated DNS server will be configured and hosted in the Network Operations Center (NOC) to provide name resolution services across the enterprise network. This server will handle forward and reverse lookup zones, ensuring that hostnames can be accurately resolved to IP addresses and vice versa. By centralizing DNS services in the NOC, we achieve better manageability, high availability, and faster resolution performance. The DNS server will be integrated with the DHCP system to support dynamic DNS updates, allowing automatic registration and removal of DNS records as IP addresses are assigned or released. Proper zone delegation and security measures (such as DNSSEC) will be implemented to ensure integrity and prevent spoofing or cache poisoning attacks. Access to the DNS server will be controlled via ACLs to comply with departmental restrictions while maintaining network efficiency.



## 9.2 DNS Accessibility

## The resource is accessible from all networks without any limitations. There are no Access Control List (ACL) restrictions applied. Connectivity is unrestricted and open across all network segments.

## 10.1 Multi-area Design

## The network uses a Backbone Area 0 as the central hub for routing. Each physical location is assigned a separate OSPF area, such as Area 1, Area 2, and so on. This design improves scalability and optimizes routing efficiency across the network.

## 10.2 Route Summarization

## Route summarization is applied at Area Border Routers (ABRs) to minimize routing table size. This reduces the number of individual routes advertised between areas. It enhances network performance and simplifies route management.

## 11.1 Subnetting with Least Wastage

## Used Variable Length Subnet Masking (VLSM) for efficient IP address planning. It allows subnets of different sizes based on host requirements. This approach optimizes IP usage and supports better network scalability.

## 11.2 Addressing Plan

## Allocated subnets based on actual user count, including a buffer for future growth. This ensured efficient IP usage tailored to real network needs. Classful addressing was avoided to maximize flexibility and scalability.

## 12. Conclusion

This network design ensures high security by implementing strict ACLs, MAC binding, and port security. Optimized routing is achieved through OSPF area segmentation, summarization, and VLSM-based IP planning. Departmental isolation is enforced using VLANs and ACLs to restrict inter-departmental access. Only essential protocols are allowed at the NOC edge, minimizing exposure to threats. Efficient IP utilization and clear traffic control contribute to overall network stability. These configurations are designed to support Mobilink’s future scalability and performance needs.