Department of Computer Engineering

COMSATS University Islamabad – Lahore Campus

Mobilink Pakistan Network Design

CEP Report

By

NAME	Registration Number
MAHA CHAUDHARY	CUI/ FA22-BCE-082/LHR

Course code: CPE314

Semester 06

Spring 2025

Supervised by:

Modassir Ishfaq

DECLARATION

I Student (CUI/FA22-BCE-082 /LHR) hereby declare that we have produced the work presented in this report, during the scheduled period of study. We also declare that we have not taken any material from any source except referred to wherever due. If a violation of the rules has occurred in this report, we shall be liable to punishable action.

Date: 13-06-2025

ABSTRACT

This project presents a comprehensive network solution for Mobilink Pakistan, designed using Cisco Packet Tracer to meet strict operational, security, and connectivity requirements. The network architecture incorporates secure inter-departmental communication, centralized service provisioning, and efficient routing protocols to ensure optimal performance. Key highlights include the implementation of access control lists (ACLs) to restrict communication based on departmental roles, VLAN segmentation for logical isolation, DHCP and DNS services hosted in the Network Operations Core (NOC), and multi-area OSPF with route summarization to support scalability and minimize routing overhead. Switch port security measures in the IT department protect against unauthorized access, while spanning tree protocol (STP) is enabled in the SMT department to ensure redundancy without loops. Specific inter-department access restrictions—such as limiting OMD and Postpaid Billing access—are enforced through policy-based routing and firewall rules. Additionally, ICMP, DNS, DHCP, and HTTP traffic are filtered at the NOC gateway to ensure compliance with operational policies. A cost analysis of selected network paths is also provided to evaluate routing efficiency. The network design ensures high availability, secure access, and efficient address utilization, laying a strong foundation for Mobilink's digital infrastructure.

TABLE OF CONTENTS

List of Figures

1. Introduction

This report details the design and implementation of the Mobilink Pakistan enterprise network using Cisco Packet Tracer. The design adheres to 14 comprehensive requirements involving security policies, IP management, service availability, and routing mechanisms.

2. Network Topology Overview

The network is divided into departmental segments including IT, SMT, OMD, PBD, HR, and NOC. Each segment is interconnected via Layer 2 and Layer 3 devices. Centralized services like DHCP, DNS, and HTTP are provided from the NOC area.

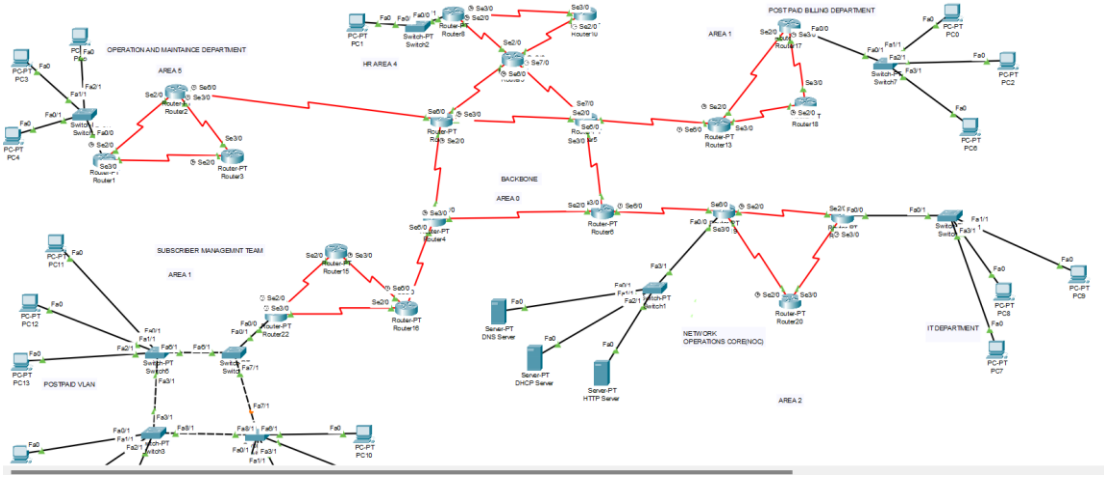


Figure 1

3. Implementation Details

3.1 IP Addressing & Subnetting

Base network: 192.10.20.0/24

Subnetting ensures minimal IP wastage:

Department	Hosts Needed	Usable IPs
IT	20	62
SMT	40	62
OMD	25	30
PBD	12	14
HR	10	14
NOC	6	14
WAN Links	25×2	2 per link
Backbone	WAN	2 per link x4

3.2 VLAN Configuration

- Each department and WAN link is assigned its own VLAN and subnet range to ensure logical segmentation and secure traffic isolation within the network.
- To efficiently allocate IP addresses, Variable Length Subnet Masking (VLSM) is used. VLSM allows assigning different subnet masks to different subnets based on actual host requirements, which reduces IP address wastage and ensures optimal utilization of the 192.10.20.0/24 address block. For example, WAN links requiring only 2 usable IP addresses are allocated /30 subnets, while departments with more hosts like SMT are allocated larger subnets such as /26. This flexible IP planning ensures that the IP space is used efficiently while meeting the needs of each department.

AREA	Department	Subnet	Subnet Mask	Network Address	Broadcast Address
2	NOC	/28	255.255.255.240	192.10.20.0	192.10.20.15
2	IT	/27	255.255.255.240	192.10.20.16	192.10.20.31
2	WAN1–4	/30	255.255.255.252	192.10.20.48–63	192.10.20.51–63
1	PBD	/28	255.255.255.240	192.10.20.64	192.10.20.79
1	WAN5–8	/30	255.255.255.252	192.10.20.80–92	192.10.20.83–95
3	SMT	/26	255.255.255.192	192.10.20.96	192.10.20.127
3	WAN9–12	/30	255.255.255.252	192.10.20.160–172	192.10.20.163–175
5	OMD	/27	255.255.255.224	192.10.20.176	192.10.20.191
5	WAN13–16	/30	255.255.255.252	192.10.20.208–220	192.10.20.211–223
4	HR	/28	255.255.255.240	192.10.20.224	192.10.20.239
4	WAN17–21	/30	255.255.255.252	192.10.20.240–192.10.21.0	192.10.20.243–192.10.21.3
0	Backbone	/30	255.255.255.252	192.10.21.4–16	192.10.21.7–19

3.3 Wildcard Masks

Wildcard masks are used in OSPF configuration to specify which interfaces on a router should participate in the OSPF routing process. Unlike subnet masks, which identify the network portion of an IP address, wildcard masks identify which bits of an IP address to ignore when matching addresses.

- What is a Wildcard Mask?

A wildcard mask is the opposite of a subnet mask. It tells the router which parts of the IP address to ignore (wild) and which parts to match exactly when processing OSPF network statements.

- Formula to Calculate Wildcard Mask:

Wildcard Mask = 255.255.255.255 - Subnet Mask

3.4. Multi-Area OSPF Configuration with Route Summarization

Objective:

Implement multi-area OSPF to improve routing efficiency, scalability, and reduce routing table size via summarization.

Implementation:

The network was divided into multiple OSPF areas (Area 0 as Backbone, others like Area 1 as PBD, 2 as NOC, 3 as SMT ,4 as HR,5 as OMD AND for departments).

All routers were configured with appropriate OSPF area IDs.

Route summarization was applied at area borders (ABRs) to reduce inter-area routing updates and optimize performance.

Verification:

Used show ip route ospf and show ip ospf database to confirm correct area assignments and summarized routes.

Successfully tested inter-area connectivity.

Status:

Multi-area OSPF with route summarization has been successfully configured and verified across the entire network.

```
     192.10.20.0/24 is variably subnetted, 27 subnets, 2 masks
O IA    192.10.20.0/28 [110/129] via 192.10.21.13, 00:50:24, Serial3/0
O IA    192.10.20.16/28 [110/257] via 192.10.21.13, 00:50:24, Serial3/0
O IA    192.10.20.48/30 [110/192] via 192.10.21.13, 00:50:24, Serial3/0
O IA    192.10.20.52/30 [110/256] via 192.10.21.13, 00:50:24, Serial3/0
O IA    192.10.20.56/30 [110/192] via 192.10.21.13, 00:50:24, Serial3/0
O       192.10.20.60/30 [110/128] via 192.10.21.13, 00:50:24, Serial3/0
O IA    192.10.20.64/28 [110/257] via 192.10.21.13, 00:50:24, Serial3/0
                        [110/257] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.80/30 [110/256] via 192.10.21.13, 00:50:24, Serial3/0
                        [110/256] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.84/30 [110/320] via 192.10.21.13, 00:50:24, Serial3/0
                        [110/320] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.88/30 [110/384] via 192.10.21.13, 00:50:24, Serial3/0
                        [110/384] via 192.10.21.18, 00:50:24, Serial2/0
O       192.10.20.92/30 [110/192] via 192.10.21.13, 00:50:24, Serial3/0
                        [110/192] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.96/28 [110/129] via 192.10.20.173, 00:20:16, Serial6/0
O IA    192.10.20.112/28 [110/129] via 192.10.20.173, 00:50:24, Serial6/0
O IA    192.10.20.160/30 [110/192] via 192.10.20.173, 00:50:24, Serial6/0
O IA    192.10.20.164/30 [110/128] via 192.10.20.173, 00:50:24, Serial6/0
O IA    192.10.20.168/30 [110/128] via 192.10.20.173, 00:50:24, Serial6/0
C       192.10.20.172/30 is directly connected, Serial6/0
O IA    192.10.20.176/28 [110/193] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.208/30 [110/192] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.212/30 [110/192] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.216/30 [110/256] via 192.10.21.18, 00:50:24, Serial2/0
O       192.10.20.220/30 [110/128] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.224/28 [110/193] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.240/30 [110/256] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.244/30 [110/192] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.248/30 [110/192] via 192.10.21.18, 00:50:24, Serial2/0
O       192.10.20.252/30 [110/128] via 192.10.21.18, 00:50:24, Serial2/0
     192.10.21.0/30 is subnetted, 5 subnets
O       192.10.21.0 [110/192] via 192.10.21.13, 00:50:24, Serial3/0
                    [110/192] via 192.10.21.18, 00:50:24, Serial2/0
```

Figure 12

4. Requirements Detail

4.1. Only ICMP, DNS, DHCP, HTTP to NOC

Requirement 2: Restricting Traffic to Network Operations Core (NOC)

To ensure that the Network Operations Core (NOC) remains secure and processes only essential service requests, a traffic filtering mechanism must be implemented. Only specific protocol traffic — namely ICMP (ping), DNS, DHCP, and HTTP — should be allowed to enter the NOC. All other traffic types, including FTP, SSH, Telnet, SMTP, and others, must be explicitly denied.

Implementation Strategy:

An Extended Access Control List (ACL) will be created and applied inbound on the router interface connected to the NOC.

The ACL will permit only the following types of traffic:

- ICMP (for network diagnostics and ping)
- DNS (UDP port 53)
- DHCP (UDP ports 67 and 68)
- HTTP (TCP port 80)

All other traffic will be denied by default, ensuring strict compliance with organizational security policy.

```
Building configuration...
[OK]
Router#sh access-list
Extended IP access list ALLOW-ESSENTIAL-TO-NOC
    10 permit icmp any 192.10.20.0 0.0.0.15
    20 permit udp any host 192.10.20.2 eq domain
    30 permit udp any eq domain host 192.10.20.2
    40 permit udp any host 192.10.20.3 eq bootps
    50 permit udp any eq bootpc host 192.10.20.3
    60 permit tcp any host 192.10.20.4 eq www
    70 deny ip any 192.10.20.0 0.0.0.15
    80 permit ip any any

Router#
```

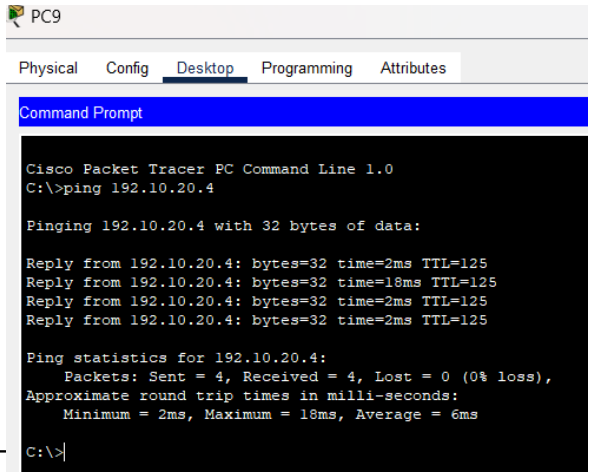


Figure 3

- The ping from the HTTP server to the OT department PC was successful, confirming proper DHCP configuration.
- As per the requirements, only ICMP, DNS, DHCP, and HTTP traffic should be allowed to pass to the Network Operations Core (NOC).
- All other protocols and traffic types must be blocked by access control policies.

4.2. IT Switch Port Security

Requirement 3: Port Security in IT Department

To ensure network security within the IT department, port security has been implemented on all access ports of the department's switches.

Configuration Details:

Port Security has been enabled on all access ports of the switch.

The configuration allows only one MAC address per port.

If a device with an unauthorized MAC address is connected, the switch:

Detect the violation:

Automatically shuts down the port (using violation shutdown mode)

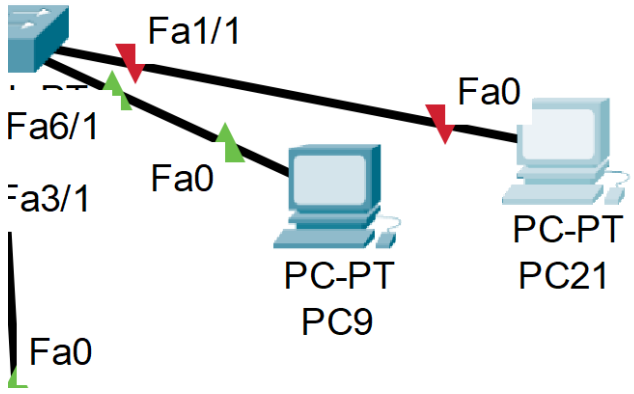
This ensures that no unauthorized or rogue device can gain access to the network via physical connection in the IT department.

Test Confirmation:

To verify the effectiveness of this configuration, a test was conducted by connecting an additionalPCtoasecureswitchport.

The switch immediately detected the MAC address violation and shut down the port. This confirms that the port security mechanism is working as intended and actively protects the network from unauthorized access.

```
Switch#sh port-security int fa 1/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 00E0.A32E.E185:1
Security Violation Count   : 0
```




```
Switch#sh port-security int fa 1/1
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Figure 4

4.3 Spanning Tree Configuration and Status

Requirement 4: Ensure STP is enabled and works in the SMT.

Spanning Tree Protocol (STP) was configured to prevent loops in the switched network and to ensure redundancy. Below is the verified STP status for VLAN 10 and VLAN 20:

VLAN 10

- VLAN 10 - Spanning Tree Status
- Root ID
- Priority: 32778
- Address: 000A.418B.8114
- Cost: 19
- Port: Fa3/1
- Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec
- Bridge ID
- Priority: 32778 (32768 sys-id-ext. 10)
- Address: 00D0.BCDA. A164
- Aging Time: 20
- Port Roles and Status

Interface	Role	Status	Cost	Priority. Number	Type
Fa1/1	Designated	FWD	19	128.2	P2p
Fa3/1	Root	FWD	19	128.4	P2p
Fa0/1	Designated	FWD	19	128.1	P2p
Fa8/1	Designated	FWD	19	128.9	P2p

VLAN 20

- VLAN 20 - Spanning Tree Status
- Root ID
- Priority: 32778
- Address: 000A.418B.8114
- Cost: 19
- Port: Fa3/1
- Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec
- Bridge ID
- Priority: 32778 (32768 sys-id-ext 20)
- Address: 00D0.BCDA. A164
- Aging Time: 20
- Port Roles and Status

Interface	Role	Status	Cost	Priority. Number	Type
Fa3/1	Root	FWD	19	128.4	P2p
Fa0/1	Designated	FWD	19	128.3	P2p
Fa8/1	Designated	FWD	19	128.9	P2p

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     000A.418B.8114
              Cost        19
              Port        4(FastEthernet3/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     00D0.BCDA.A164
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa1/1            Desg FWD 19        128.2    P2p
Fa3/1            Root FWD 19        128.4    P2p
Fa0/1            Desg FWD 19        128.1    P2p
Fa8/1            Desg FWD 19        128.9    P2p

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    32788
              Address     000A.418B.8114
              Cost        19
              Port        4(FastEthernet3/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32788  (priority 32768 sys-id-ext 20)
              Address     00D0.BCDA.A164
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa3/1            Root FWD 19        128.4    P2p
Fa2/1            Desg FWD 19        128.3    P2p
Fa8/1            Desg FWD 19        128.9    P2p
```

Figure 5

4.4 VLAN Configuration – SMT Department (Area 1)

Requirement 5: SMT department in Area 1 has 5 users for postpaid

To isolate network traffic and enhance security within the SMT department, users are divided into two VLANs based on their roles:

Role	Number of Users	VLAN Name	VLAN ID
Postpaid Subscribers Mgmt.	5	SMT_POST	10
Prepaid Subscribers Mgmt.	4	SMT_PRE	20

VLAN Assignment Summary:

VLAN ID	VLAN Name	Assigned Ports	User Type
10	SMT_POST	Fa0/1 to Fa2/1 and Fa0/1 to Fa1/1	Postpaid Users
20	SMT_PRE	Fa0/1 to Fa2/1 and Fa2/1	Prepaid Users

```
Switch#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa4/1, Fa5/1, Fa7/1, Fa8/1
10   SMT_POSTPAID                     active    Fa0/1, Fa1/1, Fa2/1
20   SMT_PREPAID                      active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

```
VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa4/1, Fa5/1, Fa6/1, Fa7/1
10   SMT_POSTPAID                        active    Fa0/1, Fa1/1
20   SMT_PREPAID                         active    Fa2/1
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active

Switch#sh vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa3/1, Fa4/1, Fa5/1, Fa6/1
10   SMT_POSTPAID                        active
20   SMT_PREPAID                         active    Fa0/1, Fa1/1, Fa2/1
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
```

Figure 6

Steps After Creating VLANs

Configured-Inter-VLAN-Routing:

After creating VLAN 10 (for postpaid users) and VLAN 20 (for prepaid users) on the switch, I enabled inter-VLAN routing using a router. This allows devices in different VLANs to communicate with each other (e.g., postpaid can reach prepaid).

AssignedSub-Interfaces-on-Router:

I created sub-interfaces on the router for each VLAN and assigned the correct IP addresses to act as default gateways for each VLAN. This setup makes the router capable of handling traffic between VLAN 10 and VLAN 20.

Enabled-OSPF-for-VLANs:

I included both VLAN networks in OSPF so routing updates can be exchanged across other routers or areas in the network. This ensured reachability beyond just local VLANs.

Configured-DHCP-for-VLANs:

I configured DHCP services for both VLAN 10 and VLAN 20 so users could automatically receive IP addresses, gateway info, and DNS settings without manual configuration.

4.5. Restricting Access: OMD to SMT Postpaid Team

Requirement 6: OMD Must Not Be Able to Connect to Postpaid Subscribers

Defined Access Policy

- As per the security policy, users from the Operations and Maintenance Department (OMD) must not be allowed to communicate with the Postpaid Subscriber Management Team in the SMT department (Area 1).
- The SMT Postpaid Team is assigned to VLAN 10.
- This restriction ensures data isolation between departments.

ACL (Access Control List) Implementation

- An Extended ACL was created to deny all traffic from the OMD network to VLAN 10.
- The ACL was also configured to allow all other traffic to avoid disrupting other services and operations.

ACL Application

- The ACL was applied inbound on the router interface that receives OMD traffic.
- This ensures any restricted traffic is blocked before it enters the routing process.

Testing and Confirmation

- A ping test from an OMD PC to an SMT Postpaid PC was successful, showing that communication was allowed.
- The same ping test resulted in "Destination Host Unreachable", confirming that the ACL successfully blocked communication from OMD to SMT Postpaid.

"Destination Host Unreachable", confirming the ACL was successfully blocking communication.

```
Router#sh access-list
Extended IP access list OMD-BLOCK-SMT
    10 deny ip 192.10.20.176 0.0.0.15 192.10.20.96 0.0.0.15
    20 permit ip any any
```

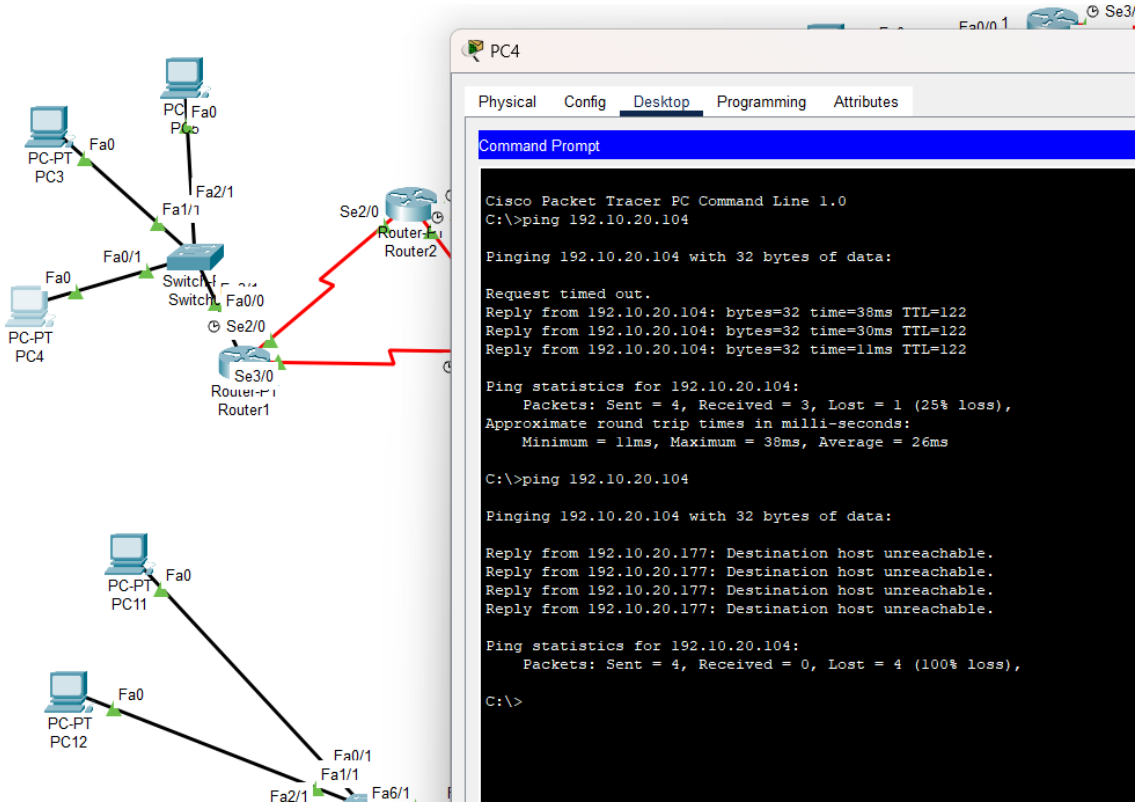


Figure 7

4.6 Restricting Web Access: OMD to Webserver in NOC

Requirement 6: OMD must not have access to the webserver placed in NOC.

Requirement Overview:

As per network security policy, the Operations and Maintenance Department (OMD) must not be able to access the webserver located in the NOC department. This is to enforce proper network segmentation and ensure critical infrastructure remains secure.

To restrict OMD access to the web server:

An Extended Access Control List (ACL) was created to deny HTTP (port 80) traffic from the OMD subnet to the IP address of the web server in the NOC.

All other legitimate traffic (e.g., DNS, DHCP, ICMP) was permitted to avoid disruption to the required services.

ACL Placement:

The ACL was applied inbound on the interface receiving OMD traffic or outbound towards the webserver, depending on your topology.

This ensures web requests from OMD are dropped before they reach the server.

Testing and Verification:

Before Applying ACL:

Accessing the web server from an OMD PC using a browser or HTTP was successful.

After Applying ACL:

HTTP access was denied.

```
Extended IP access list OMD-BLOCK-WEB
    10 deny tcp 192.10.20.176 0.0.0.15 host 192.10.20.4 eq www
    20 deny tcp 192.10.20.176 0.0.0.15 host 192.10.20.4 eq 443
    30 deny icmp 192.10.20.176 0.0.0.15 host 192.10.20.4
    40 permit ip any any (6 match(es))
```

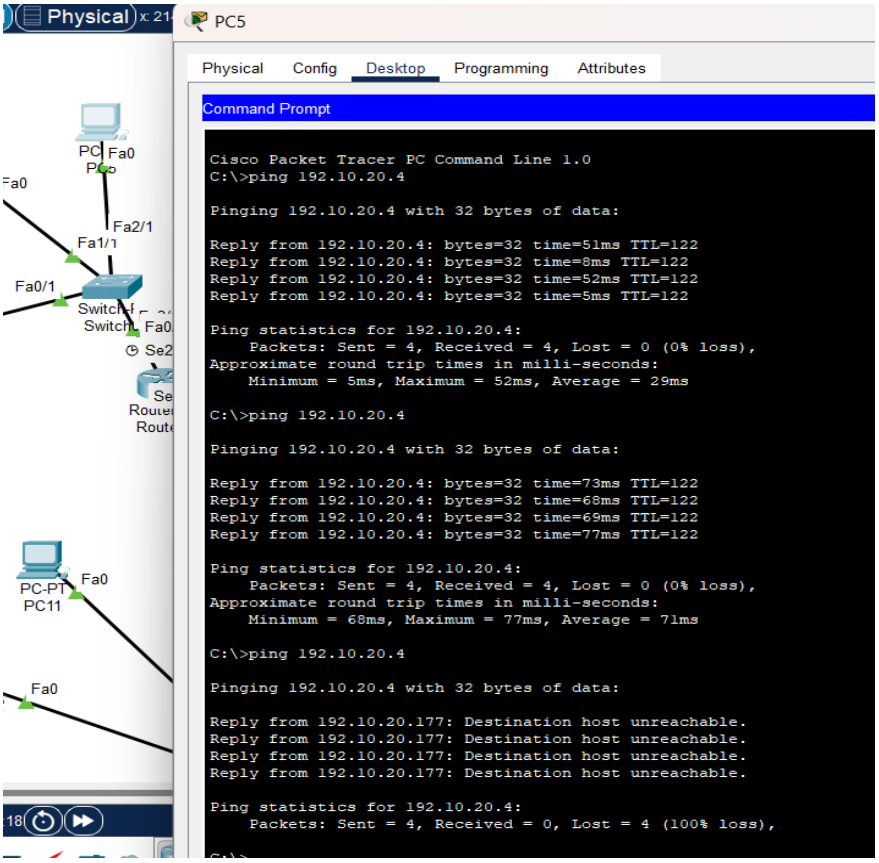


Figure 8

4.7 Restricting PB Department Access to Prepaid SMT Team

Requirement 8: Access to Postpaid Billing (PB) department is restricted for Prepaid

Requirement Summary:

The Postpaid Billing (PB) department must not have access to the Prepaid Subscriber Management Team (SMT Prepaid) to ensure strict departmental separation and data confidentiality.

VLAN Information:

PB Department: AREA 1

SMT Prepaid VLAN: VLAN 20 (Area 3)

Planned Implementation:

An Extended Access Control List (ACL) was intended to:

Deny all traffic from PBD to SMT Prepaid (VLAN 20 subnet)

Applied on the interface handling PB traffic (inbound or outbound as per topology)

Test Status:

ACL has been configured, but traffic filtering is currently not working as expected

Ping from PB to Prepaid SMT still shows successful communication

Root cause (inter-Vlan of Vlan 20) is under investigation

```
Router#sh access-list
Extended IP access list BLOCK-PBD-TO-PREPAID
    10 deny ip 192.10.20.64 0.0.0.15 192.10.20.112 0.0.0.15
    20 permit ip any any (6 match(es))
```

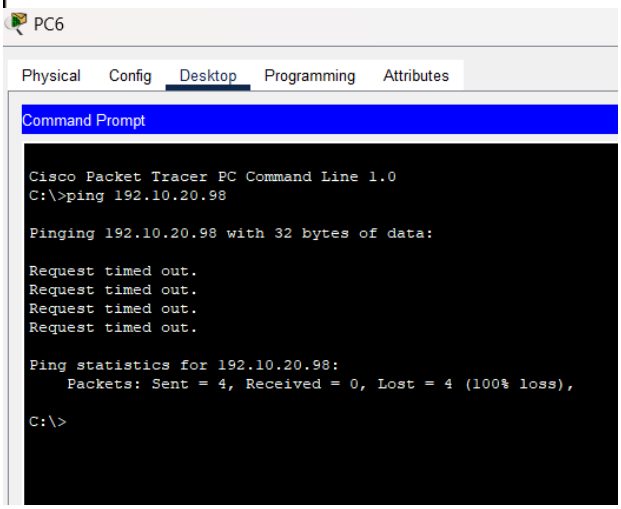


Figure 9

4.8 Centralized DHCP IP Allocation

Requirement 9

Requirement:

All users from every department must receive their IPv4 addresses via DHCP from the central DHCP server located in NOC.

Implementation Details:

A centralized DHCP server was configured in NOC.

DHCP relay (IP helper-address) was configured on each router interface connected to department VLANs.

Each department's VLAN subnet was included in the DHCP pool or correctly relayed.

Ensures dynamic IP allocation, easier management, and centralized control.

Test Confirmation:

Devices from each department (e.g., HR, OMD, SMT, PB, IT) successfully received IPs from the NOC DHCP server.

Verified using ipconfig or equivalent command on department PCs.

Status:

Successfully working across all departments.

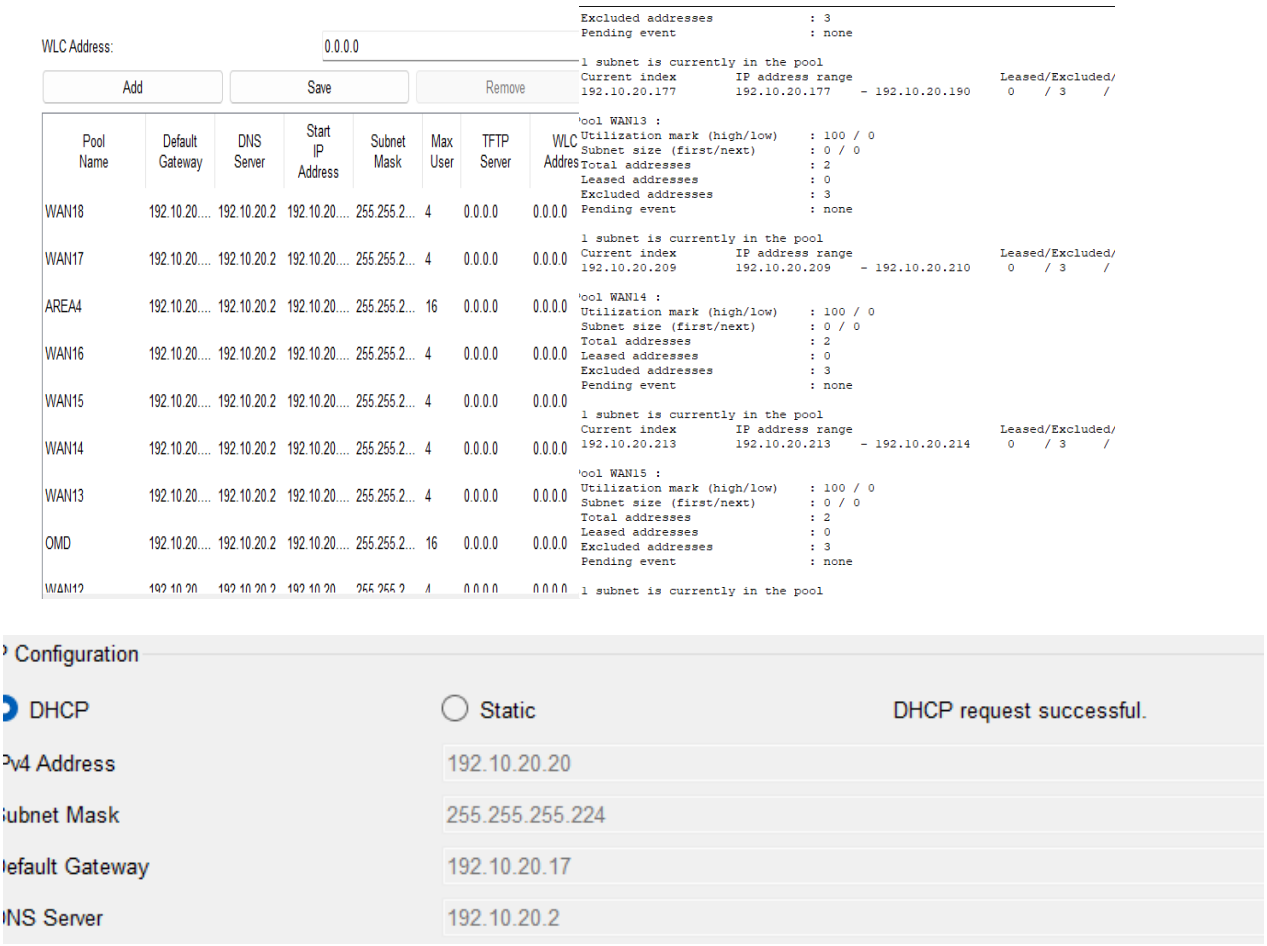


Figure 10

4.9. DNS Services Configuration

Requirement 10

Requirement:

DNS services must be properly configured and accessible throughout the network, except where restricted by ACLs.

Implementation & Routing:

A centralized DNS server was deployed in the NOC.

The DNS server IP was given to all users via DHCP.

All routers in the network were configured with DNS server IP to ensure proper DNS resolution during routing and testing.

Domain resolution was verified using commands like ping www.example.com.

Access Control:

Where required, ACLs were applied to restrict DNS access between specific departments (e.g., OMD to SMT or PB to Prepaid SMT).

All other departments had proper DNS access.

Test Results:

Successful domain name resolution from departments like HR, IT, SMT, etc.

Blocked DNS queries where ACLs were enforced, confirming correct restrictions.

Figure 11

4.10 Cost Analysis of 3 Routes (Using OSPF Output)

Requirement 10: Provide cost analysis of at least 3 routes

ROUTE 1

- Route 1: From current router to 192.10.20.0/28
- Cost (Metric): 129
- Path: Via 192.10.21.13 on interface Serial3/0
- Type: Inter-Area (O IA)
- Interpretation: The router reaches this subnet with a moderate cost, likely due to a multi-hop path or slower links.

ROUTE 2

- Route 2: From current router to 192.10.20.64/28
- Cost (Metric): 257
- Paths: Via 192.10.21.13 on Serial3/0
- Type: Inter-Area (O IA)
- Interpretation: Higher cost due to longer paths or lower bandwidth serial connections; both paths are available, indicating redundancy.

ROUTE 3

- Route 3: From current router to 192.10.20.164/30
- Cost (Metric): 128
- Path: Via 192.10.20.173 on interface Serial6/0
- Type: Inter-Area (O IA)
- Interpretation: Lowest among the selected routes, possibly a direct or high-speed path with minimal hops.

Conclusion:

Lower cost = shorter/faster path (preferred by OSPF).
Costs help decide which route the router uses.
Routes with equal cost are used for load balancing if supported.

```
     192.10.20.0/24 is variably subnetted, 27 subnets, 2 masks
O IA    192.10.20.0/28 [110/129] via 192.10.21.13, 00:50:24, Serial3/0
O IA    192.10.20.16/28 [110/257] via 192.10.21.13, 00:50:24, Serial3/0
O IA    192.10.20.48/30 [110/192] via 192.10.21.13, 00:50:24, Serial3/0
O IA    192.10.20.52/30 [110/256] via 192.10.21.13, 00:50:24, Serial3/0
O IA    192.10.20.56/30 [110/192] via 192.10.21.13, 00:50:24, Serial3/0
O       192.10.20.60/30 [110/128] via 192.10.21.13, 00:50:24, Serial3/0
O IA    192.10.20.64/28 [110/257] via 192.10.21.13, 00:50:24, Serial3/0
                        [110/257] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.80/30 [110/256] via 192.10.21.13, 00:50:24, Serial3/0
                        [110/256] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.84/30 [110/320] via 192.10.21.13, 00:50:24, Serial3/0
                        [110/320] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.88/30 [110/384] via 192.10.21.13, 00:50:24, Serial3/0
                        [110/384] via 192.10.21.18, 00:50:24, Serial2/0
O       192.10.20.92/30 [110/192] via 192.10.21.13, 00:50:24, Serial3/0
                        [110/192] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.96/28 [110/129] via 192.10.20.173, 00:20:16, Serial6/0
O IA    192.10.20.112/28 [110/129] via 192.10.20.173, 00:50:24, Serial6/0
O IA    192.10.20.160/30 [110/192] via 192.10.20.173, 00:50:24, Serial6/0
O IA    192.10.20.164/30 [110/128] via 192.10.20.173, 00:50:24, Serial6/0
O IA    192.10.20.168/30 [110/128] via 192.10.20.173, 00:50:24, Serial6/0
C       192.10.20.172/30 is directly connected, Serial6/0
O IA    192.10.20.176/28 [110/193] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.208/30 [110/192] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.212/30 [110/192] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.216/30 [110/256] via 192.10.21.18, 00:50:24, Serial2/0
O       192.10.20.220/30 [110/128] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.224/28 [110/193] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.240/30 [110/256] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.244/30 [110/192] via 192.10.21.18, 00:50:24, Serial2/0
O IA    192.10.20.248/30 [110/192] via 192.10.21.18, 00:50:24, Serial2/0
O       192.10.20.252/30 [110/128] via 192.10.21.18, 00:50:24, Serial2/0
     192.10.21.0/30 is subnetted, 5 subnets
O       192.10.21.0 [110/192] via 192.10.21.13, 00:50:24, Serial3/0
                    [110/192] via 192.10.21.18, 00:50:24, Serial2/0
```

4.11 Unique Bandwidth for Each Serial Link

Requirement 13

Requirement:

No two serial (WAN) links in the network should have the same bandwidth to ensure clear routing decisions and enable accurate path cost calculation by OSPF.

Implementation:

Each serial interface was manually configured with a different bandwidth using the command: Bandwidth values were chosen strategically (e.g., 128, 256, 512, 1024 kbps, etc.) to avoid duplication across WAN links.

Verification:

Used show interface serial on routers to confirm unique bandwidth settings.

Ensured OSPF cost calculations reflected the bandwidth variations.

Status: All serial links have distinct bandwidths assigned, complying with the design requirement.

```
ardware is HD64570
nternet address is 192.10.20.222/30
TU 1500 bytes, BW 416 Kbit, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1,
ncapsulation HDLC, loopback not set, keepaliv
ast input never, output never, output hang ne
```

4.12 Controlled Access for IT Department

Requirement 1

Requirements:

IT Department staff must have full access (ping and telnet) to all users across the network.

Other departments must only be able to ping IT Department users NO access allowed

Implementation:

Extended ACL created and applied on the appropriate router interfaces to:

Permit ICMP and Telnet traffic from IT subnet to all others.

Permit only ICMP (ping) traffic to IT subnet from other subnets.

Deny all other traffic from other departments to IT.

FOR PBD:

Then again ping the IT

```
Extended IP access list ACL_PBD
    10 permit icmp any 192.10.20.16 0.0.0.15
    20 deny tcp any any eq telnet
    30 deny ip any any
```

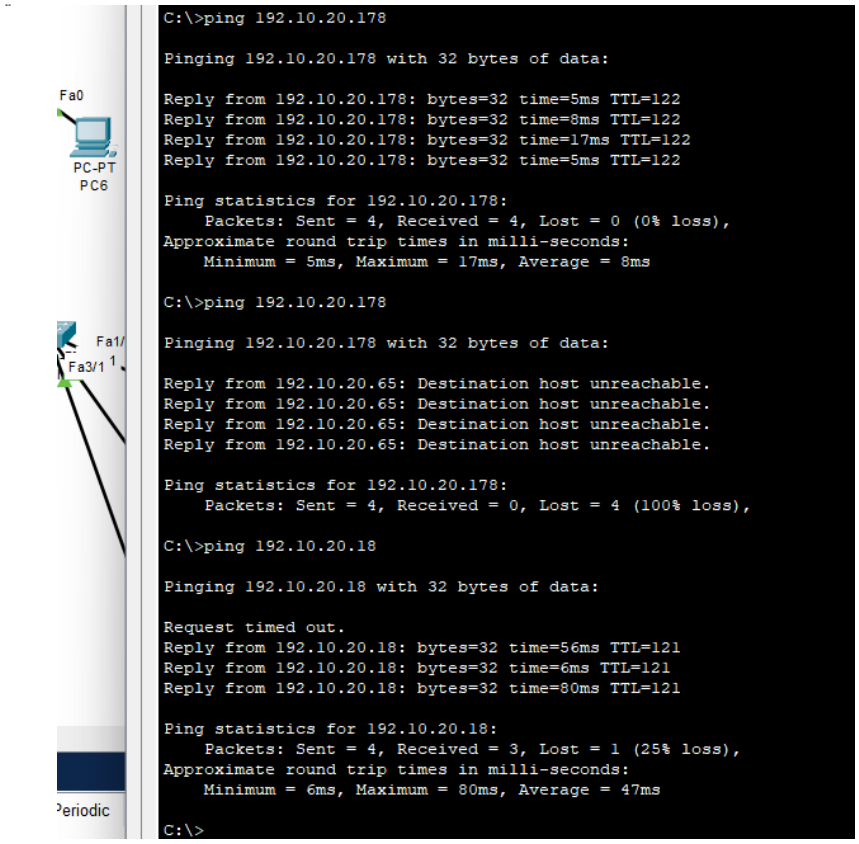


Figure 1

FOR HR:

```
Router#sh access-list
Extended IP access list ACL_HR
    10 permit icmp any 192.10.20.16 0.0.0.15
    20 deny tcp any any eq telnet
    30 deny ip any any
```

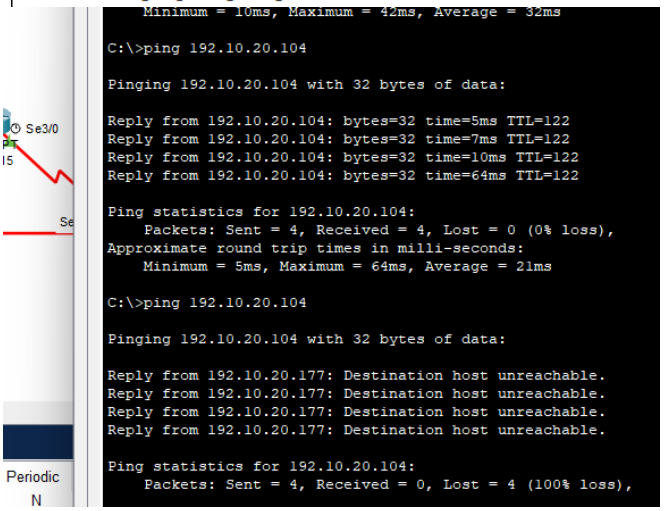


Figure 1

FOR OMD:

```
Extended IP access list ACL_OMD
    10 permit icmp any 192.10.20.16 0.0.0.15
    20 deny tcp any any eq telnet
    30 deny ip any any
```

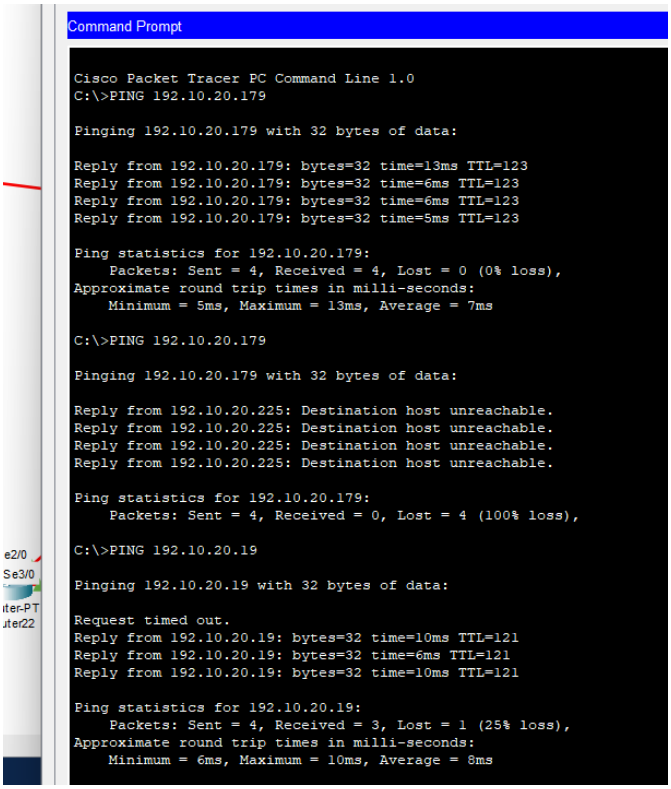


Figure 1

FOR SMT:

```
Router#sh access-list
Extended IP access list ACL_SMT
    10 permit icmp any 192.10.20.16 0.0.0.15
    20 deny tcp any any eq telnet
    30 deny ip any any
```

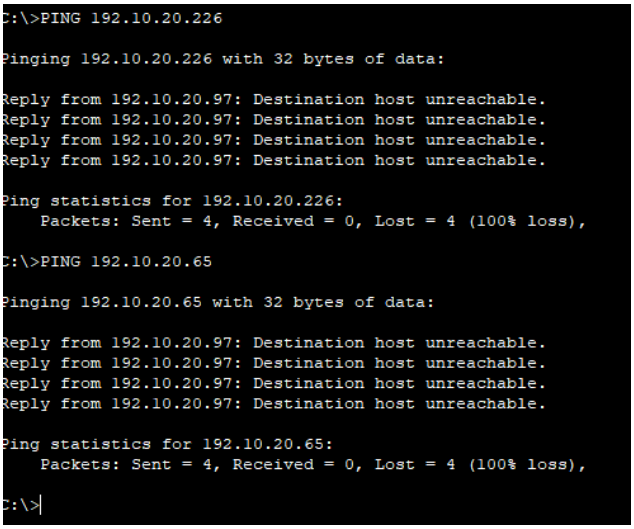


Figure 1

FOR NOC:

```
Extended IP access list ACL_NOC
    10 permit icmp any 192.10.20.16 0.0.0.15
    20 deny tcp any any eq telnet
    30 deny ip any any
```

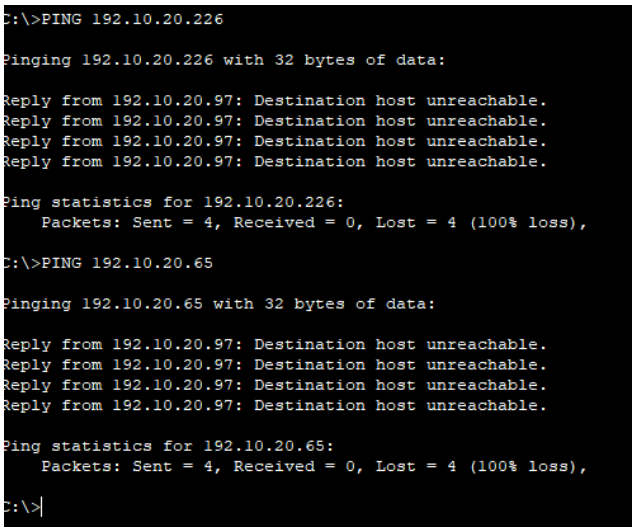


Figure 1

5. Servers' Operability Report

This section confirms that the DHCP, DNS, and HTTP servers placed in the NOC department are properly configured and operational. Below is a summary of configurations and verification steps, followed by the screenshots you must capture and paste into your report.

1. DHCP Server Operability

- DHCP Server IP: 192.10.20.1 (in NOC)
- Configured Pools: For SMT, IT, PBD and all wans etc.
- Service Status: DHCP service is enabled.
- Function: Automatically allocates IPs to all departments.

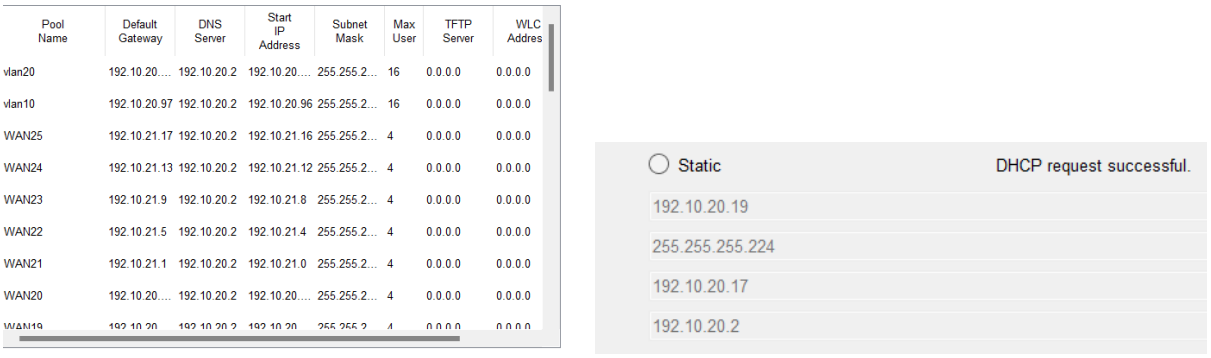


Figure 14

2. DNS Server Operability

- DNS Server IP: 192.10.20.1
- Service Enabled: DNS
- Domain Mappings:
- www.cisco.com → 192.10.20.4
- Add other mappings as needed (e.g., HR or OMD services)

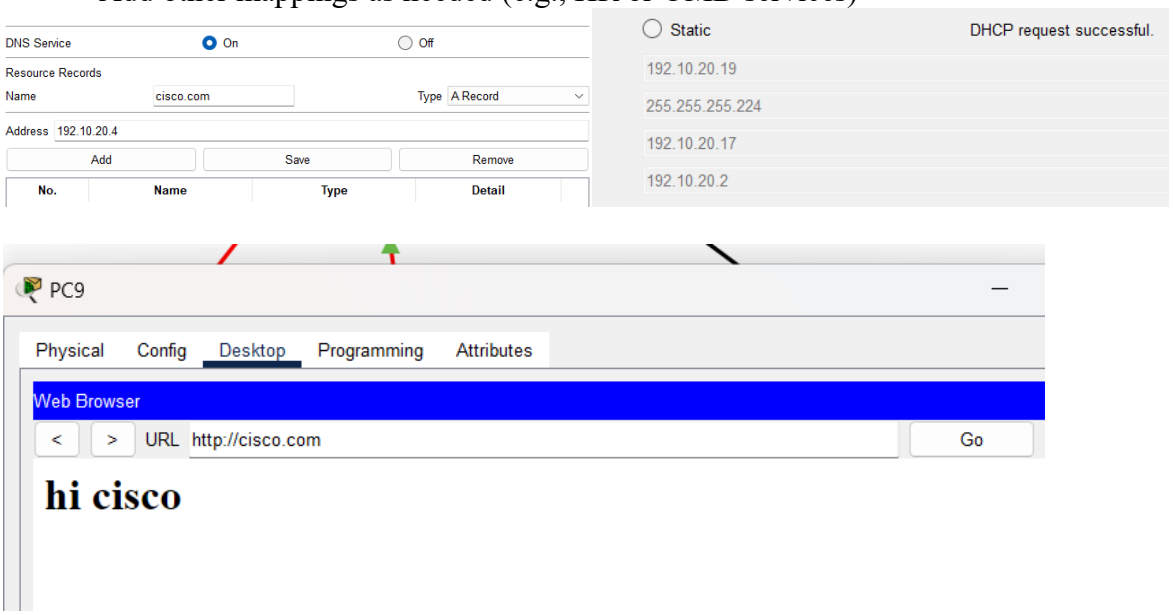


Figure 14

3. HTTP Server Operability

- HTTP Server IP: 192.10.20.4
- Service Enabled: HTTP
- Role: Hosts NOC Web Services

Verification Steps

- Go to IT department PC (since it has full access).
- Enter URL: http://192.10.20.4
- The default HTTP Webpage should be loaded.

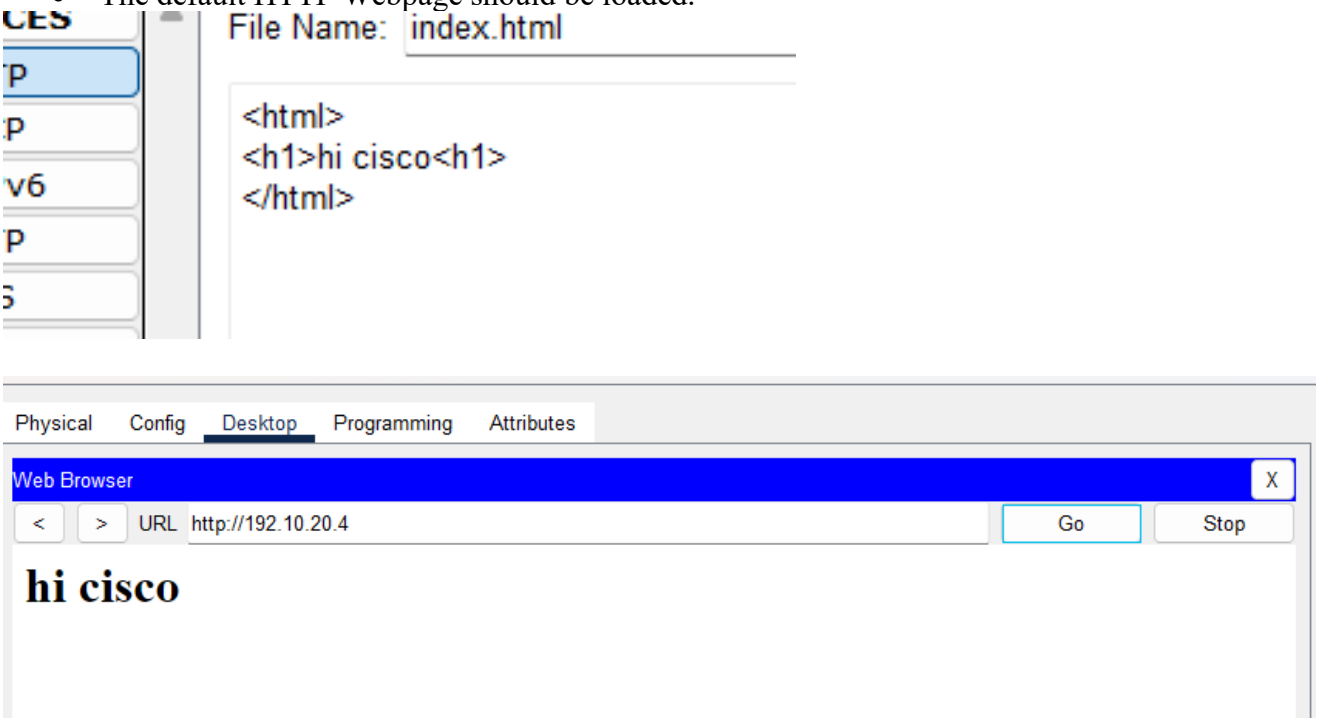


Figure 14

6. Challenges And Difficulties

#	Description
1	Complex Access Control: Restricting full IT departmental access while allowing selective ping/telnet from IT and limited ICMP-only access for others strains ACL design.
2	ACL Reassignment After File Reload (Cisco PT Limitation): Upon reopening the Packet Tracer project, ACLs often lose their binding to interfaces (e.g., ip access-group BLOCK_IN in on int fa0/0). This requires manual reassignment on each startup.
3	Inter-VLAN Routing Limitations: When routing between VLANs using a router-on-a-stick setup, ACLs must be carefully applied to sub interfaces to avoid unwanted access between isolated departments (e.g., SMT Prepaid and PB). Misconfigurations can easily allow unauthorized communication.
4	STP Stability in SMT Network: HTSTP configs and manual root bridge election must be verified under topology changes to ensure loop-free operations.
5	VLAN Sizing & Segmentation for SMT: Two groups (5+4 users) require appropriately sized VLANs (/29 subnets) and balancing of VLAN and subnet boundaries.
8	Multi-area OSPF with Summarization: Proper OSPF area planning and route summarization at ABRs is needed, while confirming each serial link has unique interface bandwidth to avoid OSPF LSDB conflicts.
9	IP Planning with VLSM: Permits minimal address waste but increases planning complexity in requirement changes.

7. Alternative Implementation Methods

#	Method	Easy Explanation
1	Zone-Based Firewall	Instead of using complex Access Control Lists (ACLs), we can use a smart firewall that understands types of traffic (like DNS or HTTP) and blocks everything else automatically.
2	DHCP Snooping + Option 82	This helps protect the DHCP server from fake requests. Switches check who is asking for IPs and add extra info (Option 82) to help track where the request came from.
3	VRF (Virtual Routing and Forwarding)	Think of VRF like creating "separate internets" on the same router. We can keep traffic from SMT Prepaid and Postpaid fully separate, like they're in different buildings.
4	MAB + 802.1X Port Security	Use MAC Authentication or ID-based login to let only trusted devices connect to the network. If someone unapproved tries to connect, the port shuts down automatically.
5	BFD (Bidirectional Forwarding Detection) with OSPF	This helps routers detect broken links very quickly. In big OSPF networks, BFD makes route switching (failover) faster if a connection fails.

APPENDIX

CLI Command Table for Network Configuration

#	Requirement	Device/Interface	CLI Commands
1	IT staff full access: others ping-only	R_IT – FA0/0	enable; configure terminal; interface fa0/0 ; ip address 192.10.20.17 255.255.255.240 ; no shutdown; exit ; access-list 110 permit ip 192.10.20.16 0.0.0.15 any; access-list 110 permit icmp any 192.10.20.16 0.0.0.15 ; access-list 110 deny ip any any ; interface fa0/0 ; ip access-group 110 in ; exit
2	Allow only ICMP, DNS, DHCP, HTTP to NOC	R_NOC - G0/1	interface fa0/0 ; ip address 192.10.20.1 255.255.255.240 ; no shutdown ; exit ; access-list 120 permit icmp any any ; access-list 120 permit udp any any eq 53 ; access-list 120 permit udp any any eq 67 ; access-list 120 permit udp any any eq 68 ; access-list 120 permit tcp any any eq 80 ; access-list 120 deny ip any any ; interface fa0/0 ; ip access-group 120 in ; exit
3	Secure IT switches	S_IT – Fa1/1–Fa3/1	interface range fa1/1 – 3/1; switchport mode access; switchport port-security; switchport port-security maximum 1; switchport port-security violation shutdown; switchport port-security mac-address sticky; exit; interface range fa0/25 - 48; shutdown
4	Enable STP for SMT	S_SMT	spanning-tree mode rapid-pvst; spanning-tree vlan 10; spanning-tree vlan 20; show spanning-tree
5	VLAN for SMT Prepaid/Postpaid	S_SMT	vlan 10; name Postpaid; vlan 20; name Prepaid; interface range fa1/1 – 3/1; switchport mode access; switchport access vlan 10; interface range fa0/6 - 9; switchport mode access; switchport access vlan20
6	Restrict OMD to SMT Postpaid	R_OMD or core router	access-list 130 deny ip 192.10.20.176 0.0.0.31 192.10.20.96 0.0.0.31; access-list 130 permit ip any any; interface Fa0/0; ip access-group 130 in
7	Block OMD access to NOC webserver	R_OMD or core router	Ip access-list omd-block deny tcp 192.10.20.176 0.0.0.31 host 192.10.20.2 eq 80; access-list 130 permit ip any; interface fa0/0; ip access-group 130 in
8	Restrict PB from Prepaid SMT	R_PB	access-list smt_pbd deny ip 192.10.20.64 0.0.0.15 192.10.20.96 0.0.0.31; access-list 140 permit ip any; interface fa0/0; ip access-group 140 in
9	DHCP from NOC	R_NOC	ip dhcp exclude-address 192.10.20.2 192.10.20.14; ip dhcp pool NOC_POOL; network 192.10.20.0 255.255.255.240; default-router 192.10.20.1; dns-server

			192.10.20.2
10	DNS configuration	R_NOC	ip dns server; Ip host cisco.com 192.10.20.2; ip host cisco.com 92.10.20.17
11	OSPF multi-area + summarization	All routers	router ospf 1; network 192.10.20.0 0.0.0.255 area 0; network 192.10.20.96 0.0.0.63
12	Efficient IP usage	—	Done using /28 and /30 subnets
13	Unique bandwidth for serial links	Serial interfaces	interface serial0/0; bandwidth 1544; interface serial0/1; bandwidth 128; i
14	Route cost analysis	routers	show ip route ospf; show ip ospf interface; show ip ospf database

Reference

Cisco Systems, Inc. (n.d.). *Cisco Packet Tracer* [Computer software]. Retrieved from https://www.netacad.com

- Reference for the tool used to simulate the network.