Computer Network Project

Created By: **IJ Baig**

Submission Date: **20 May 2025**

Topic: **Real Life Network Simulation using Packet Tracer**

-

📘 Project Overview

This project simulates a medium-to-large scale enterprise network using Cisco Packet Tracer, built entirely on Class C private IP addressing (192.168.x.x) with CIDR-based subnetting. The network includes multiple routers, switches, PCs, servers, and IoT devices, organized into different LAN segments. It incorporates key networking services such as DHCP, DNS, NAT, VLANs, and ACLs. Dynamic routing protocols ensure full connectivity between subnets, while ACLs and NAT are used to control access between public and private zones. A DNS server resolves custom domain names to internal services, and a DHCP server automates IP assignments. This setup closely resembles a real-world corporate network, demonstrating essential concepts in routing, security, and network service management.

IP Table:

IP table represent Devices interface IP address on specific interface subnet use in interface and Role of a specific interface in network

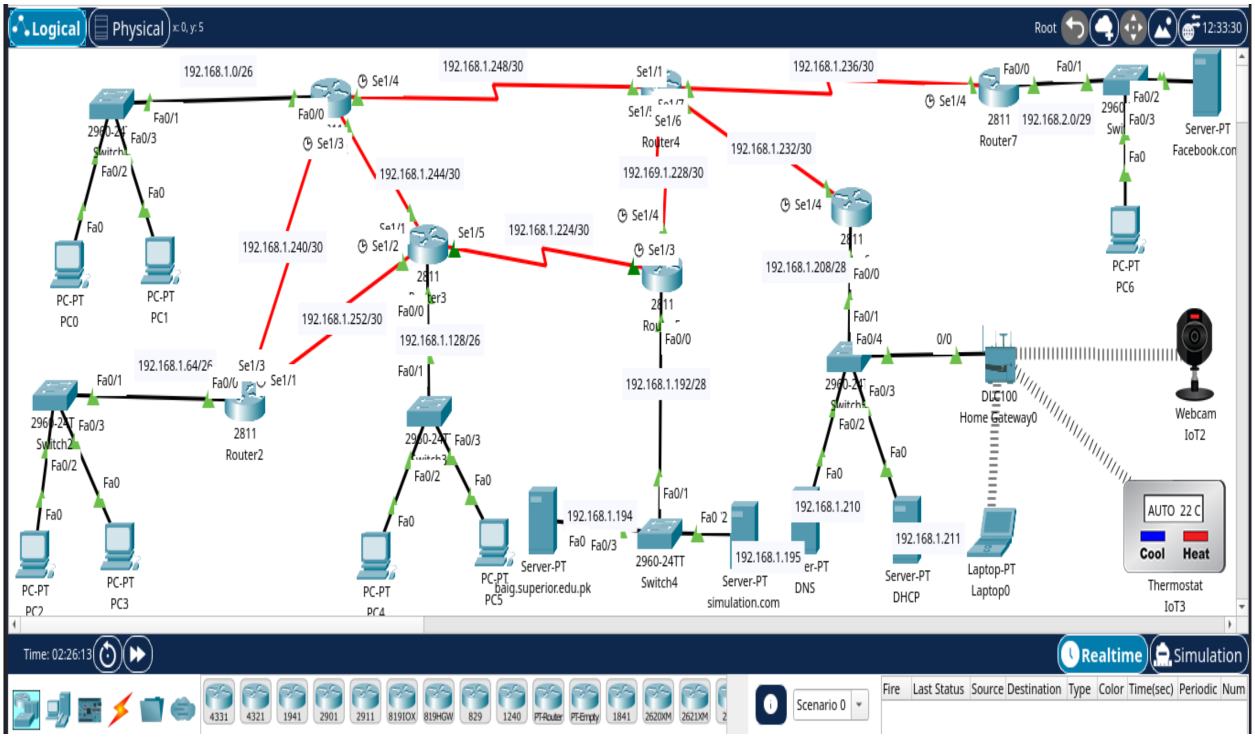
Device	Interface	IP Address	Subnet	**Role / Notes**
R1	Fa0/0	192.168.1.1	192.168.1.0/26	LAN Gateway (PCs, Switch 1)
	S1/2 (to R2)	192.168.1.241	192.168.1.240/30	Router link to R2
	S1/3 (to R3)	192.168.1.245	192.168.1.244/30	Router link to R3
	S1/4 (to R4)	192.168.1.249	192.168.1.248/30	Router link to R4
R2	Fa0/0	192.168.1.65	192.168.1.64/26	LAN Gateway (PCs, Switch 2)
	S1/1 (to R1)	192.168.1.242	192.168.1.240/30	Router link to R1
	S1/3 (to R3)	192.168.1.253	192.168.1.252/30	Router link to R3
R3	Fa0/0	192.168.1.129	192.168.1.128/26	LAN Gateway (PCs, Switch 3)
	S1/1 (to R1)	192.168.1.246	192.168.1.244/30	Router link to R1
	S1/2 (to R2)	192.168.1.254	192.168.1.252/30	Router link to R2
	S1/5 (to R5)	192.168.1.225	192.168.1.224/30	Router link to R5
R4	S1/1 (to R1)	192.168.1.250	192.168.1.248/30	Router link to R1
	S1/5 (to R5)	192.168.1.229	192.168.1.228/30	Router link to R5
	S1/6 (to R6)	192.168.1.233	192.168.1.232/30	Router link to R6
	S1/7 (to R7)	192.168.1.237	192.168.1.236/30	Router link to R7
R5	Fa0/0	192.168.1.193	192.168.1.192/28	Internal Web Server LAN

	S1/3 (to R3)	192.168.1.226	192.168.1.224/30	Router link to R3
	S1/4 (to R4)	192.168.1.230	192.168.1.228/30	Router link to R4
R6	Fa0/0	192.168.1.209	192.168.1.208/28	IoT, DHCP, DNS LAN
	S1/4 (to R4)	192.168.1.234	192.168.1.232/30	Router link to R4
R7	Fa0/0 (Public)	192.168.2.1	192.168.2.0/29	Public Side Gateway / NAT Outside
	S1/4 (to R4)	192.168.1.238	192.168.1.236/30	Router link to R4
Public Server	Fa0/0	192.168.2.2	192.168.2.0/29	Simulated Internet Server
Public PC	Fa0/0	192.168.2.3	192.168.2.0/29	Simulated Public Client
Internal Web Server 1	Fa0	192.168.1.194	192.168.1.192/28	Hosted behind R5, optional NAT
Internal Web Server 2	Fa0	192.168.1.195	192.168.1.192/28	Hosted Behind R5,
DNS Server	Fa0	192.168.1.210	192.168.1.208/28	Hosted Behind R6
DHCP Server	Fa0	192.168.1.211	192.168.1.208/28	Hosted behind R6

Reserved NAT IPs (Static Mapping Table)

Public IP	Internal IP	Purpose
192.168.2.4	192.168.1.194	NAT for Internal Web Server
192.168.2.5	192.168.1.195	NAT for Internal web Server

Topology:



🛠️ 1. Network Topology Summary

- **Total Routers:** 7
- **Total Switches:** 5
- **Client PCs:** Multiple
- **Servers:** Internal Web Server, DNS, DHCP, and Public Web Server
- **IoT Devices:** Webcam, Thermostat
- **Routing Protocol Used:** Dynamic (e.g., EIGRP or OSPF)
- **NAT:** Configured at R7 to translate internal private addresses to public

- **ACLs:** Applied on R7 to restrict external access to internal devices
- **Subnetting:** CIDR-based variable-length subnetting for optimized usage

🌐 2. Network Architecture Design

🔄 Routing:

- Dynamic routing protocol (e.g., OSPF) is configured between routers.
- Each router advertises its directly connected subnets.
- Static routes are also configured for backup paths if dynamic fails.

📡 Subnetting:

- Used **CIDR** to efficiently divide Class C range (192.168.1.0/24) into variable subnets (/30 for router links, /28 and /26 for LANs).
- A separate **/29** public IP subnet (192.168.2.0/29) is used for NAT and external devices.

📁 DHCP:

- DHCP server on R6 dynamically assigns IP addresses to client PCs.
- Lease includes subnet mask, default gateway, and DNS server.

🌐 DNS:

- DNS server on R6 resolves internal domain: baig.superior.edu.pk
- Forward and reverse DNS configured and tested via ping and browser.

🌐 Web Services:

- Internal web server hosts your assigned web page.

- Public web server simulates the internet.
- NAT maps the internal server's IP to a public IP for outside access.

🧱 VLANs:

- VLANs separate departments/clients within the LAN.
- Inter-VLAN routing is handled by the router-on-a-stick approach or Layer 3 switches (if applicable).

🔒 ACLs:

- **Inbound ACL on R7 (public gateway):**
  - Allows traffic **only to web servers** (internal IP .194).
  - Denies all other external attempts to access internal network.

🌉 NAT:

- Static NAT at R7 maps:
  - 192.168.2.4 ⟶ 192.168.1.194 (internal web server)

📷 3. Network Functionality Verification

✅ Ping Tests:

- PCs successfully ping:
  - Their own IP
  - Default Gateway
  - Remote routers
  - Servers (internal and public)

🛰️ Traceroute:

- Shows multiple hops through routers between client and web server.
- Each hop represents a router interface.
- Verifies end-to-end routing and correct paths.

🌐 DNS Lookup Test:

- Browser opens baig.superior.edu.pk
- Browser opens simulation.com
- Browser opens facebook.com
- DNS resolves to internal IP
- Successful HTTP connection to Web Server

🧪 4. Advanced Services

Service	Device	Function
DHCP	R6	Assigns IP, mask, gateway, DNS to clients
DNS	R6	Resolves web URLs
WEB	Server @ .194 and .195	Hosts internal website
NAT	R7	Allows internal web server to be accessed publicly
ACL	R7	Blocks all traffic except allowed services
IoT	Gateway0	Includes webcam and thermostat communication

🧩 5. Security Measures

- ACLs prevent unauthorized public access.

- NAT ensures internal IPs are hidden from the public.
- VLANs separate sensitive areas from general client traffic.

📌 6. Limitations & Future Improvements

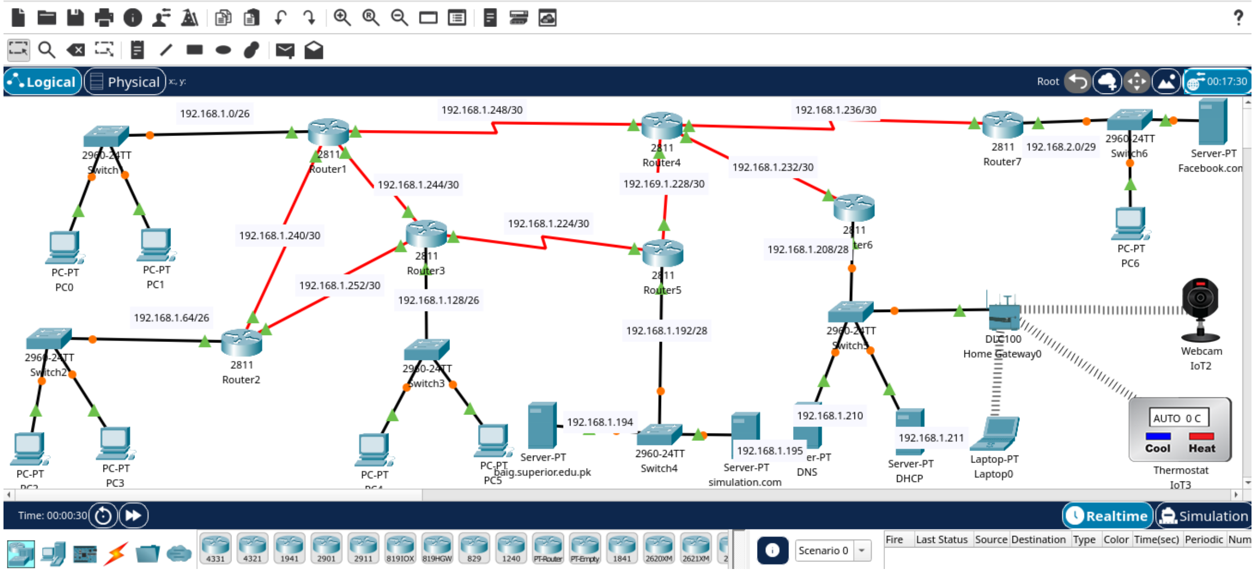
- Could integrate VPN for secure remote access.
- Upgrade to Layer 3 switches for faster inter-VLAN routing.
- Introduce backup DNS and DHCP services.

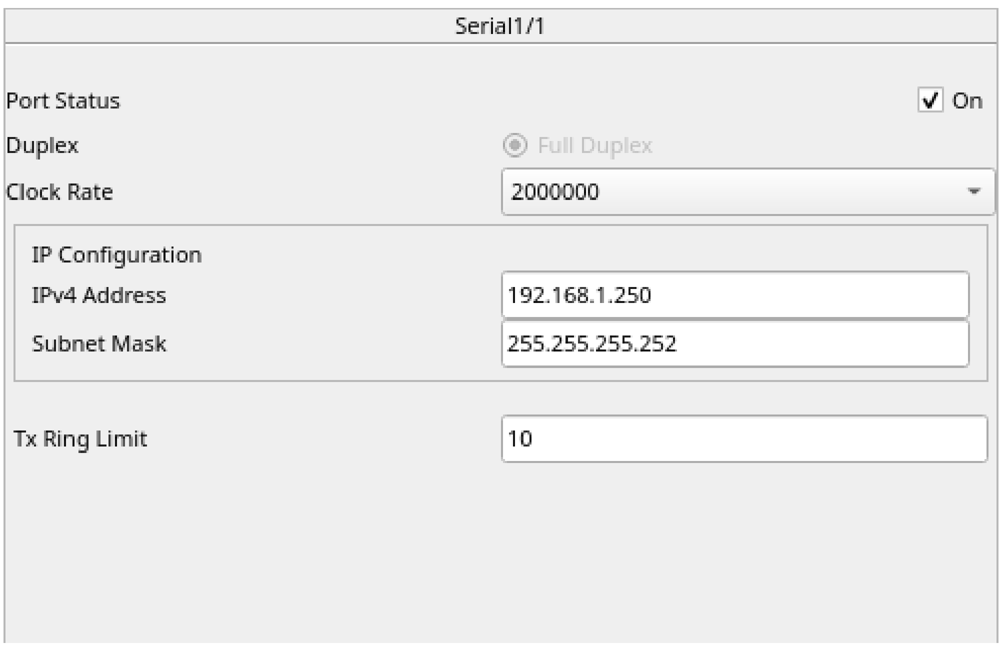
📸 7. Screenshots

Task 1 - Setting up a Network [20 marks]

Perform the following activities and support your workings with screenshots:

1. Configure the PCs, Server and Router with network addressing;





2. Configure any classless dynamic routing protocol on the routers;

OSPF is configured

```
Router#show ip route ospf
     192.168.1.0/24 is variably subnetted, 17 subnets, 4 masks
O       192.168.1.0 [110/65] via 192.168.1.249, 00:03:09, Serial1/1
O       192.168.1.64 [110/129] via 192.168.1.249, 00:02:59, Serial1/1
O       192.168.1.128 [110/129] via 192.168.1.230, 00:02:59, Serial1/5
                      [110/129] via 192.168.1.249, 00:02:59, Serial1/1
O       192.168.1.192 [110/65] via 192.168.1.230, 00:02:59, Serial1/5
O       192.168.1.208 [110/65] via 192.168.1.234, 00:03:09, Serial1/6
O       192.168.1.224 [110/128] via 192.168.1.230, 00:02:59, Serial1/5
O       192.168.1.240 [110/128] via 192.168.1.249, 00:03:09, Serial1/1
O       192.168.1.244 [110/128] via 192.168.1.249, 00:03:09, Serial1/1
O       192.168.1.252 [110/192] via 192.168.1.230, 00:02:59, Serial1/5
                      [110/192] via 192.168.1.249, 00:02:59, Serial1/1
     192.168.2.0/29 is subnetted, 1 subnets
O       192.168.2.0 [110/65] via 192.168.1.238, 00:03:09, Serial1/7

Router#show ip route
```

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.238 to network 0.0.0.0

     192.168.1.0/24 is variably subnetted, 17 subnets, 4 masks
O       192.168.1.0/26 [110/65] via 192.168.1.249, 00:03:15, Serial1/1
O       192.168.1.64/26 [110/129] via 192.168.1.249, 00:03:05, Serial1/1
O       192.168.1.128/26 [110/129] via 192.168.1.230, 00:03:05, Serial1/5
                         [110/129] via 192.168.1.249, 00:03:05, Serial1/1
O       192.168.1.192/28 [110/65] via 192.168.1.230, 00:03:05, Serial1/5
O       192.168.1.208/28 [110/65] via 192.168.1.234, 00:03:15, Serial1/6
O       192.168.1.224/30 [110/128] via 192.168.1.230, 00:03:05, Serial1/5
C       192.168.1.228/30 is directly connected, Serial1/5
L       192.168.1.229/32 is directly connected, Serial1/5
C       192.168.1.232/30 is directly connected, Serial1/6
L       192.168.1.233/32 is directly connected, Serial1/6
C       192.168.1.236/30 is directly connected, Serial1/7
L       192.168.1.237/32 is directly connected, Serial1/7
O       192.168.1.240/30 [110/128] via 192.168.1.249, 00:03:15, Serial1/1
O       192.168.1.244/30 [110/128] via 192.168.1.249, 00:03:15, Serial1/1
C       192.168.1.248/30 is directly connected, Serial1/1
L       192.168.1.250/32 is directly connected, Serial1/1
O       192.168.1.252/30 [110/192] via 192.168.1.230, 00:03:05, Serial1/5
                         [110/192] via 192.168.1.249, 00:03:05, Serial1/1
     192.168.2.0/29 is subnetted, 1 subnets
O       192.168.2.0/29 [110/65] via 192.168.1.238, 00:03:15, Serial1/7
S*   0.0.0.0/0 [1/0] via 192.168.1.238

Router#
```

3. On

any client,

ping the client's own network interfaces:

```
C:\>ping 192.168.1.67

Pinging 192.168.1.67 with 32 bytes of data:

Reply from 192.168.1.67: bytes=32 time<1ms TTL=128
Reply from 192.168.1.67: bytes=32 time<1ms TTL=128
Reply from 192.168.1.67: bytes=32 time<1ms TTL=128
Reply from 192.168.1.67: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

local router gateway:

```
C:\>ping 192.168.1.65

Pinging 192.168.1.65 with 32 bytes of data:

Reply from 192.168.1.65: bytes=32 time<1ms TTL=255
Reply from 192.168.1.65: bytes=32 time<1ms TTL=255
Reply from 192.168.1.65: bytes=32 time=1ms TTL=255
Reply from 192.168.1.65: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

the remote router interface:

```
C:\>ping 192.168.1.241

Pinging 192.168.1.241 with 32 bytes of data:

Reply from 192.168.1.241: bytes=32 time=1ms TTL=254
Reply from 192.168.1.241: bytes=32 time=36ms TTL=254
Reply from 192.168.1.241: bytes=32 time=21ms TTL=254
Reply from 192.168.1.241: bytes=32 time=20ms TTL=254

Ping statistics for 192.168.1.241:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 36ms, Average = 19ms

C:\>
```

the servers:

```
C:\>ping baig.superior.edu.pk

Pinging 192.168.1.194 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.194: bytes=32 time=2ms TTL=125
Reply from 192.168.1.194: bytes=32 time=73ms TTL=125
Reply from 192.168.1.194: bytes=32 time=67ms TTL=125

Ping statistics for 192.168.1.194:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 73ms, Average = 47ms

C:\>
```

4. Use the traceroute command from the client to the server. Include results of the traceroute in your submission, explaining meaning of traceroute output.

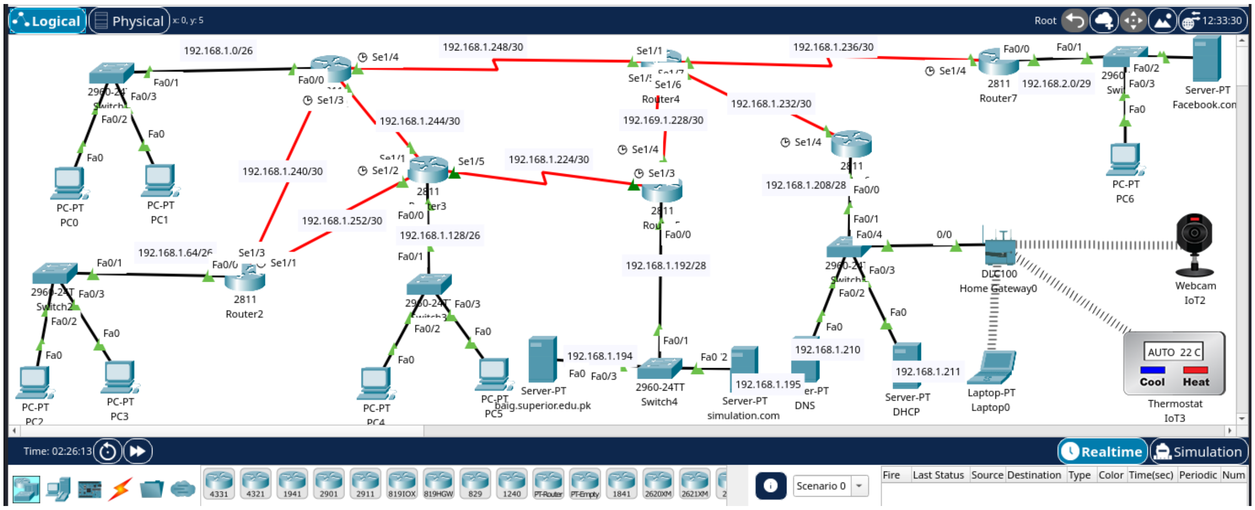
```
C:\>tracert baig.superior.edu.pk

Tracing route to 192.168.1.194 over a maximum of 30 hops:

  1   1 ms      0 ms      0 ms      192.168.1.65
  2   0 ms      22 ms     0 ms      192.168.1.254
  3   1 ms      1 ms      60 ms     192.168.1.226
  4   53 ms     0 ms      1 ms      192.168.1.194

Trace complete.

C:\>
```

Explanation:

- **Hop 1:** 192.168.1.65 — This is the local router (Router 2) serving as the default gateway for the client PC. The packet is first sent here.
- **Hop 2:** 192.168.1.254 — The packet then reaches Router 3, which connects multiple subnets and forwards traffic toward the web server's network.
- **Hop 3:** 192.168.1.226 — This is Router 5, which directly connects to the web server's LAN.
- **Hop 4:** 192.168.1.194 — The final destination, which is the web server hosting baig.superior.edu.pk.

Task 2 - Configuring Network Services [60 marks]:

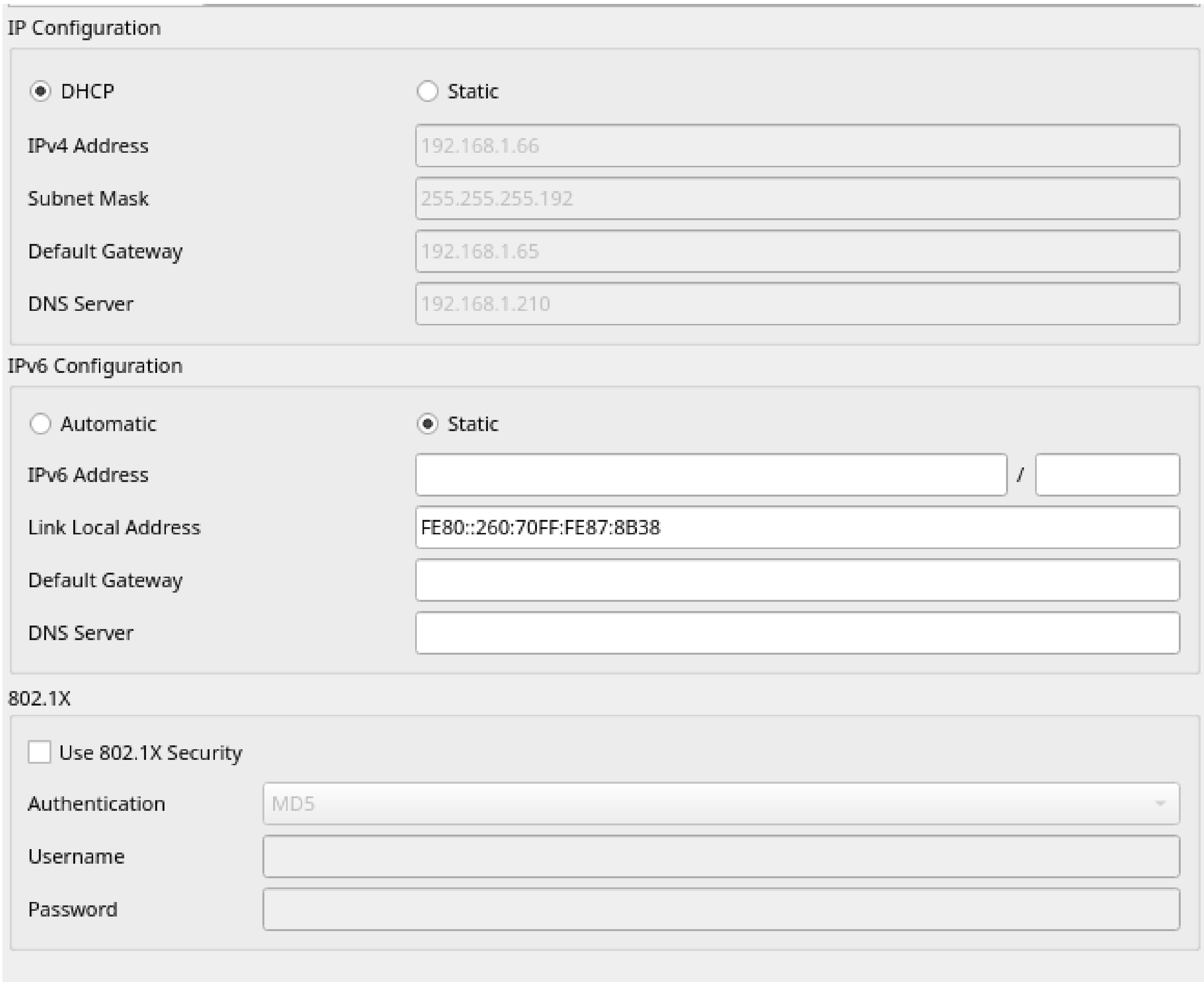
1. Subnetting: Subnet your network as per the requirements.



2. DHCP: Configure DHCP servers:

Add	Save	Remove

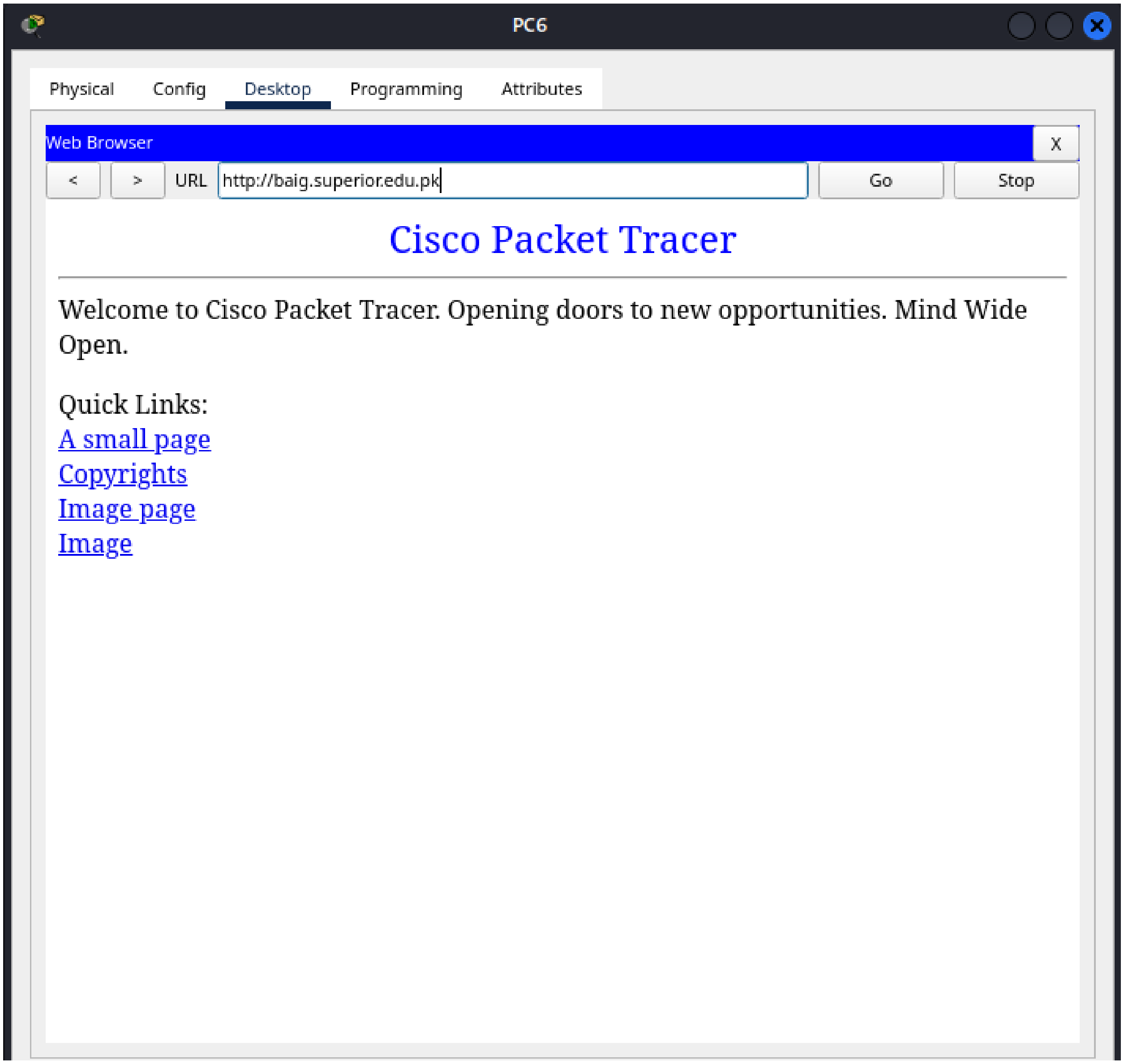
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server
Router3-Pool	192.168.1.129	192.168.1.210	192.168.1.130	255.255.255.192	60	0.0.0.0
Router2-Pool	192.168.1.65	192.168.1.210	192.168.1.66	255.255.255.192	60	0.0.0.0
Router1-Pool	192.168.1.1	192.168.1.210	192.168.1.2	255.255.255.192	60	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.1.208	255.255.255.240	512	0.0.0.0



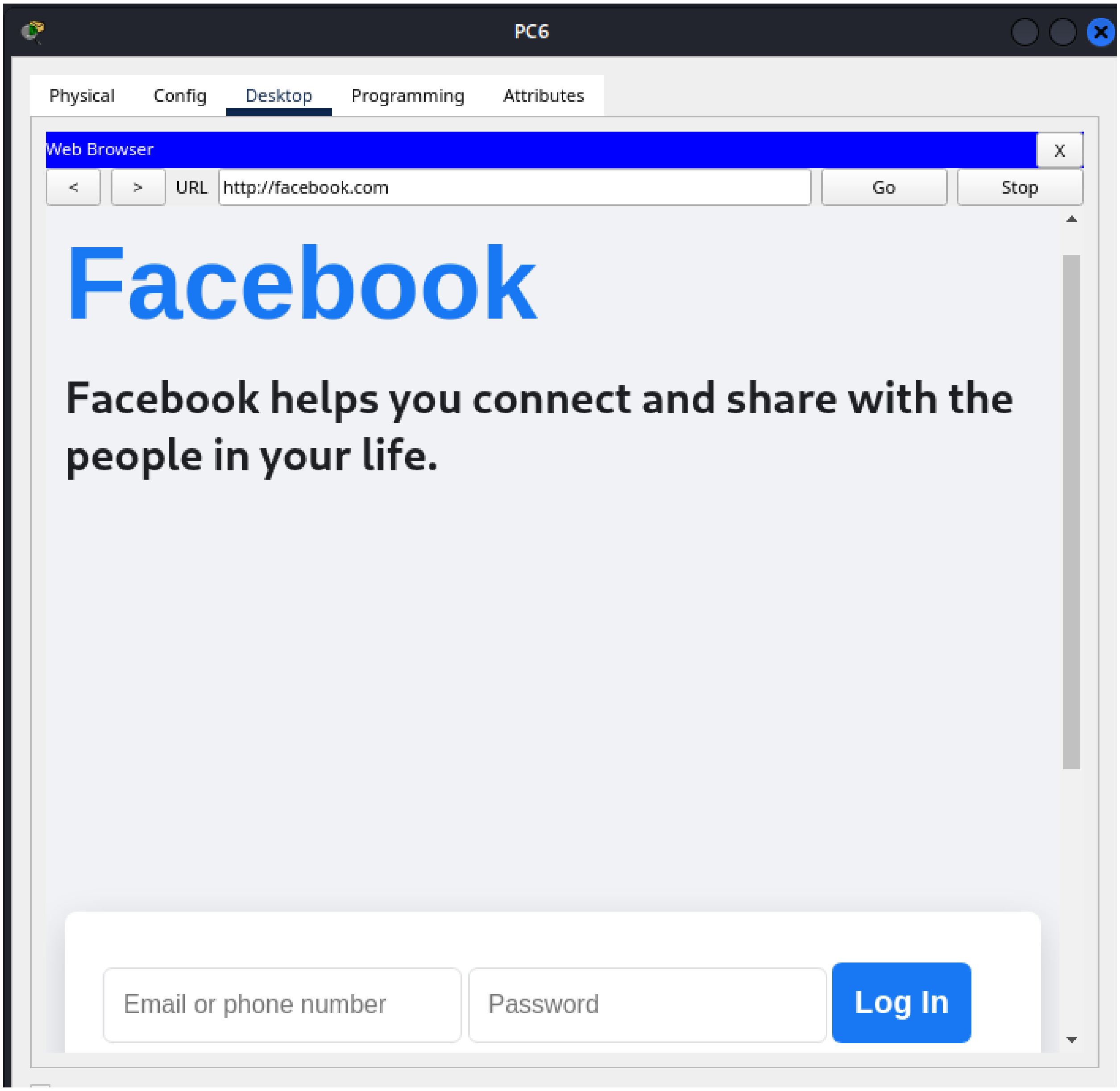
3. WEB Server:

3 web servers are attached 2 are in private network and facebook.com is in public network

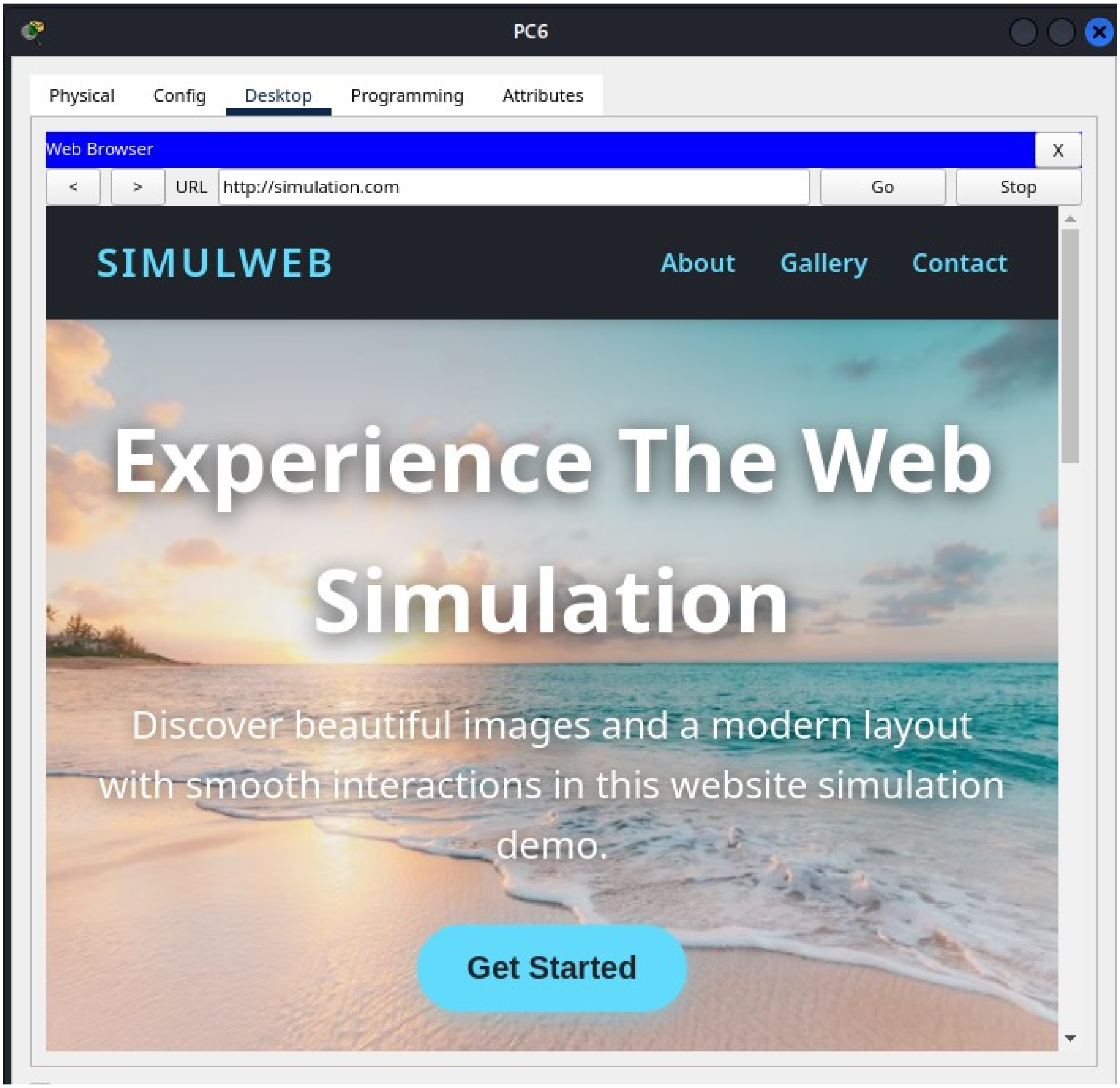
yourname.superior.edu.pk



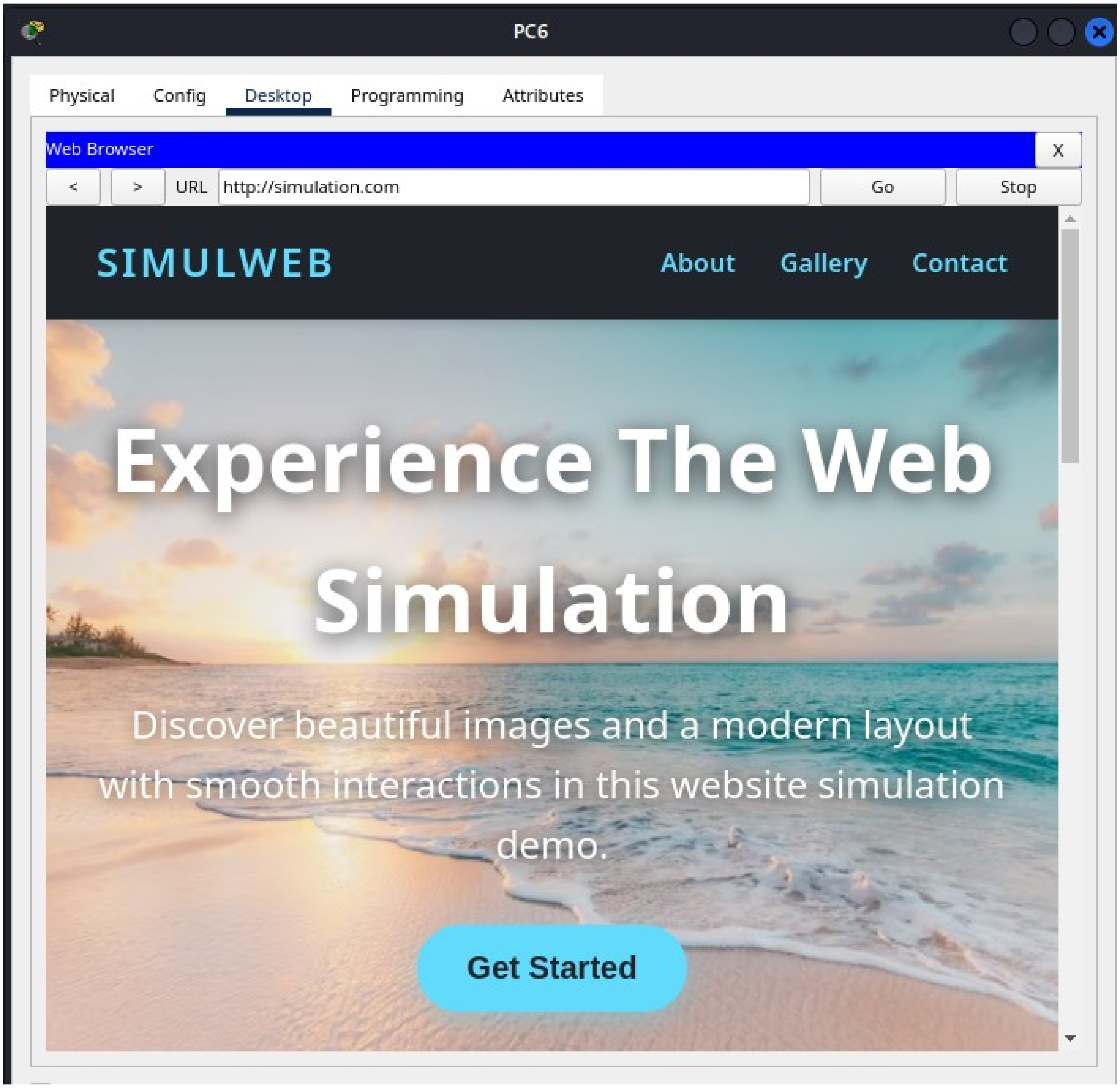
facebook.com



simulation.com

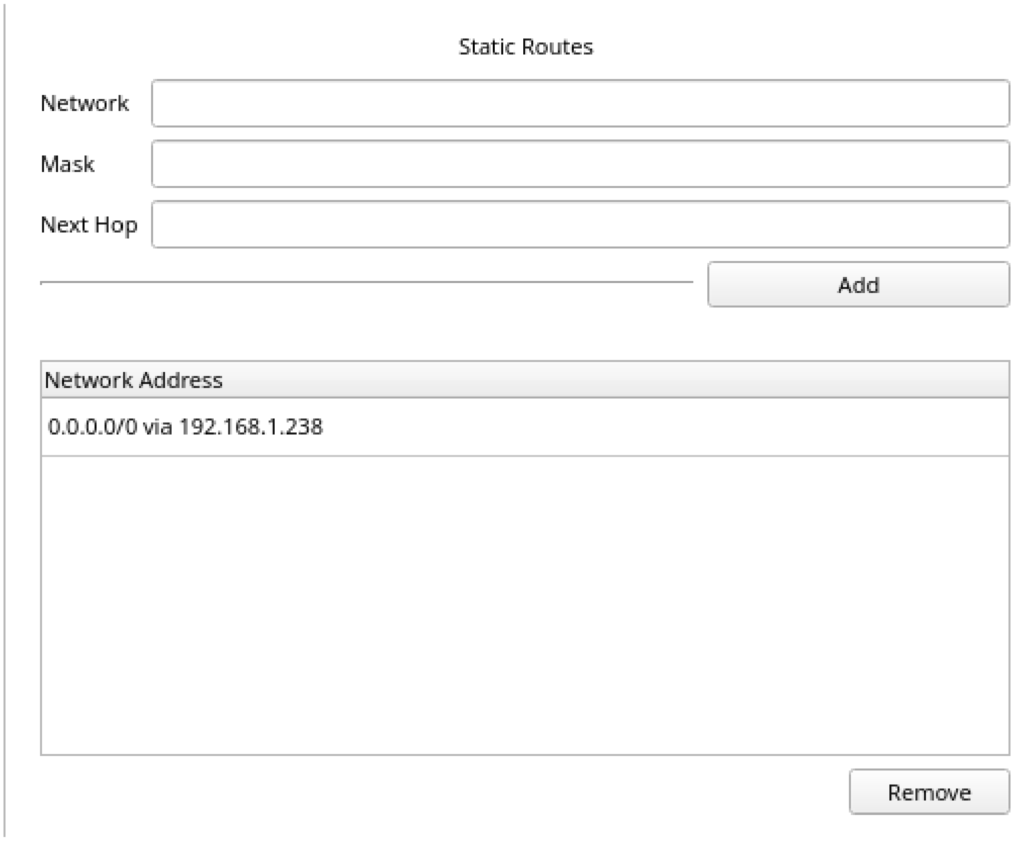


4. DNS: Configure DNS Servers



5. Routing: Configure

Static routes



dynamic routing

```
Router#show ip route ospf
     192.168.1.0/24 is variably subnetted, 17 subnets, 4 masks
O       192.168.1.0 [110/65] via 192.168.1.249, 00:03:09, Serial1/1
O       192.168.1.64 [110/129] via 192.168.1.249, 00:02:59, Serial1/1
O       192.168.1.128 [110/129] via 192.168.1.230, 00:02:59, Serial1/5
                      [110/129] via 192.168.1.249, 00:02:59, Serial1/1
O       192.168.1.192 [110/65] via 192.168.1.230, 00:02:59, Serial1/5
O       192.168.1.208 [110/65] via 192.168.1.234, 00:03:09, Serial1/6
O       192.168.1.224 [110/128] via 192.168.1.230, 00:02:59, Serial1/5
O       192.168.1.240 [110/128] via 192.168.1.249, 00:03:09, Serial1/1
O       192.168.1.244 [110/128] via 192.168.1.249, 00:03:09, Serial1/1
O       192.168.1.252 [110/192] via 192.168.1.230, 00:02:59, Serial1/5
                      [110/192] via 192.168.1.249, 00:02:59, Serial1/1
     192.168.2.0/29 is subnetted, 1 subnets
O       192.168.2.0 [110/65] via 192.168.1.238, 00:03:09, Serial1/7
```

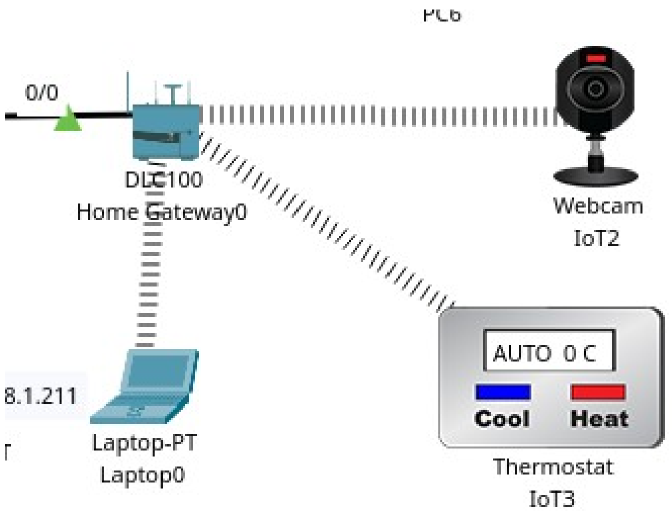
7. NAT/PAT: Configure NAT

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 192.168.2.4:80     192.168.1.194:80   ---                ---
tcp 192.168.2.4:80     192.168.1.194:80   192.168.2.3:1025   192.168.2.3:1025
tcp 192.168.2.5:80     192.168.1.195:80   ---                ---
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1030   192.168.2.3:1030
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1031   192.168.2.3:1031
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1033   192.168.2.3:1033
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1034   192.168.2.3:1034
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1035   192.168.2.3:1035
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1036   192.168.2.3:1036
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1037   192.168.2.3:1037
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1038   192.168.2.3:1038
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1039   192.168.2.3:1039
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1040   192.168.2.3:1040
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1041   192.168.2.3:1041
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1042   192.168.2.3:1042
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1043   192.168.2.3:1043
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1046   192.168.2.3:1046
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1047   192.168.2.3:1047
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1048   192.168.2.3:1048
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1049   192.168.2.3:1049
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1050   192.168.2.3:1050
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1051   192.168.2.3:1051
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1052   192.168.2.3:1052
tcp 192.168.2.5:80     192.168.1.195:80   192.168.2.3:1053   192.168.2.3:1053
```

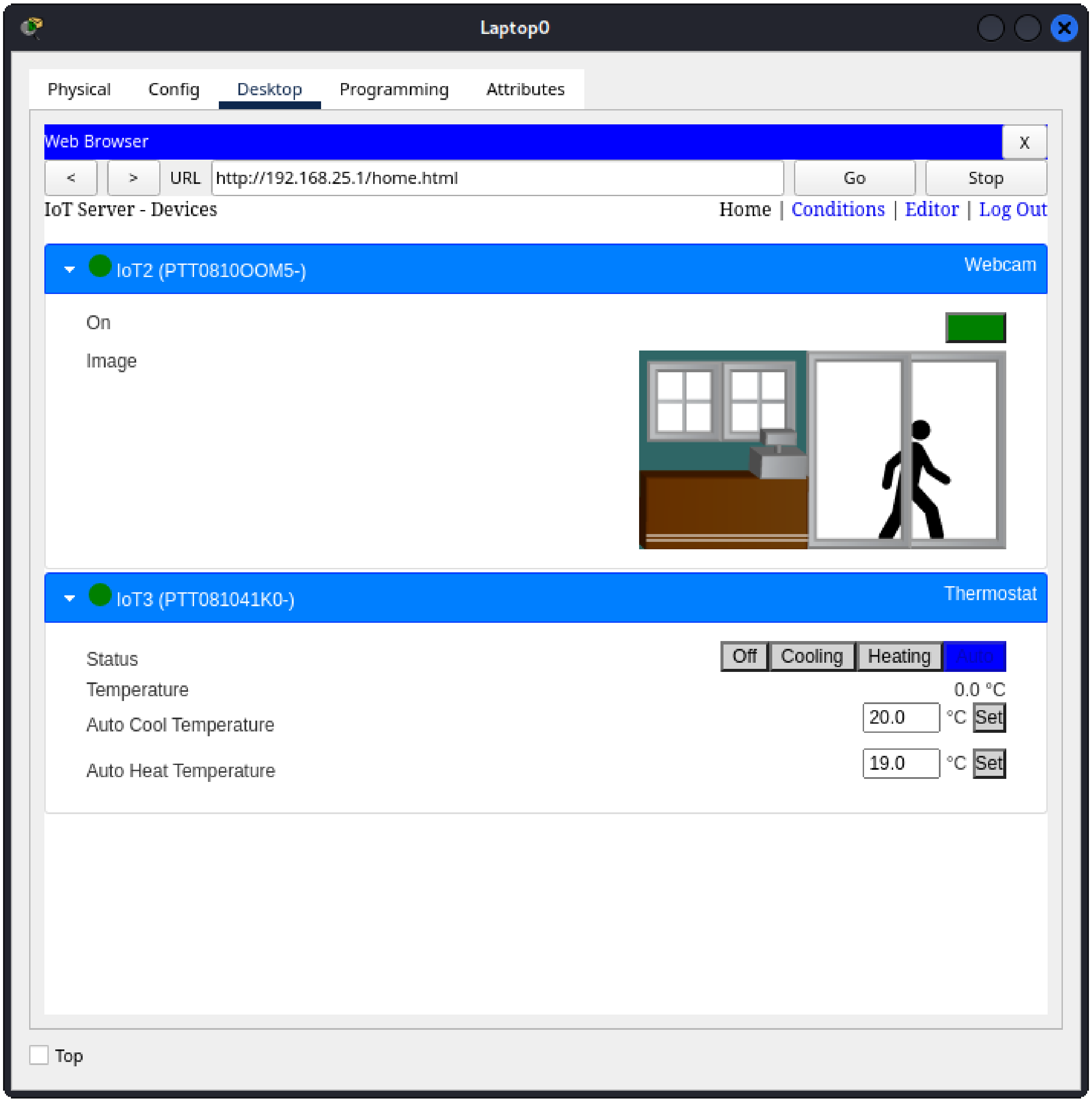
8. ACLs:

```
Router#show access-lists
Extended IP access list 100
    10 permit tcp any host 192.168.2.4 eq www (5 match(es))
    20 permit tcp any host 192.168.2.5 eq www (1423 match(es))
    30 permit tcp host 192.168.2.2 any established
    40 deny ip any any (36 match(es))

Router#
```

9. IoT Devices: Add IoT devices in your network


PC6
0/0
DLC100
Home Gateway0
Webcam
IoT2
AUTO 0 C
Cool
Heat
Thermostat
IoT3
8.1.211
Laptop-PT
Laptop0


Web Browser
X
<
>
URL
http://192.168.25.1
Go
Stop
Home Gateway Login
Username:
Password:
Submit


Laptop0
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://192.168.25.1/home.html
Go
Stop
IoT Server - Devices
Home | Conditions | Editor | Log Out
IoT2 (PTT0810OOM5-)
Webcam
On
Image
IoT3 (PTT081041K0-)
Thermostat
Status
Off
Cooling
Heating
Temperature
0.0 °C
Auto Cool Temperature
20.0
°C
Set
Auto Heat Temperature
19.0
°C
Set
Top

Task 3 [20 marks]

Write a reflective discussion around how you accomplished task 1 and task 2.

This section presents a detailed reflection and discussion of the steps undertaken to accomplish Task 1 and Task 2 of the networking project. The aim was to design and configure a complex enterprise network using Cisco Packet Tracer, incorporating essential networking services and protocols. Below is a breakdown of the activities completed, along with personalized insights and explanations for each.

✨ Task 1: Setting up the Network

1. Configuring PCs, Servers, and Router Interfaces:

All end devices, including PCs, servers, and routers, were configured with IP addresses as per the IP Addressing Plan using CIDR. Subnetting was carefully planned to optimize IP usage and network segmentation. For example, router-to-router links were configured with /30 subnets, while client LANs used /26 or /28 subnets. Each router's interface was assigned as the default gateway for the connected subnet.

2. Implementing Classless Dynamic Routing Protocol:

The dynamic routing protocol used was OSPF, as it supports classless routing and allows for efficient hierarchical design. OSPF areas were kept simple with Area 0 for the backbone. Each router was configured to advertise directly connected networks.

Commands Used:

Router(config)# router ospf 1

Router(config-router)# network 192.168.1.0 0.0.0.255 area 0

Router(config-router)# network 192.168.2.0 0.0.0.7 area 0

3. Verifying Network Connectivity:

Pings were performed from a client PC to its own IP, then to the default gateway, then to a remote router interface, and finally to the web servers. All pings were successful, confirming that OSPF was working and that end-to-end network connectivity was complete.

4. Traceroute Command Output and Explanation:

Using the tracert command, we traced the path from the client PC to the internal web server baig.superior.edu.pk. The traceroute confirmed each hop through intermediate routers. Latency values at each hop were within expected limits, confirming efficient routing and no packet drops.

```
C:\>tracert baig.superior.edu.pk

Tracing route to 192.168.1.194 over a maximum of 30 hops:

  1   1 ms     0 ms     0 ms     192.168.1.65

  2   0 ms    22 ms     0 ms     192.168.1.254

  3   1 ms     1 ms    60 ms     192.168.1.226

  4  53 ms     0 ms     1 ms     192.168.1.194

Trace complete.
```

This output shows each router hop until reaching the server. It validates both routing accuracy and performance.

💡 Task 2: Configuring Network Services

1. Subnetting:

CIDR subnetting was used to break down the 192.168.1.0/24 network into multiple /30, /28, and /26 subnets. This allowed fine-grained allocation of IPs and reduced wastage.

2. DHCP Configuration:

A DHCP server was placed in the 192.168.1.208/28 subnet and configured to serve clients with dynamic IPs, gateways, and DNS.

Commands Used:

DHCP(config)# ip dhcp pool CLIENT_POOL

DHCP(config-dhcp)# network 192.168.1.208 255.255.255.240

DHCP(config-dhcp)# default-router 192.168.1.209

DHCP(config-dhcp)# dns-server 192.168.1.210

3. Web Server Setup:

Three web servers were deployed:

- baig.superior.edu.pk on IP 192.168.1.194 (internal)
- simulation.com on a second internal server
- facebook.com on a public server with IP 192.168.2.2 These were tested successfully using browser access and DNS resolution.

4. DNS Configuration:

DNS was hosted internally to resolve domain names to respective server IPs. Forward and reverse DNS lookups were validated.

5. Static + Dynamic Routing:

While OSPF was used for dynamic routing, a few static routes were added where needed (e.g., toward NAT paths).

6. NAT/PAT Configuration:

R7 handled NAT. Internal Web Server 192.168.1.194 was mapped to public IP 192.168.2.4. This ensured the web server was accessible from the public side.

Commands Used:

R7(config)# ip nat inside source static 192.168.1.194 192.168.2.4

7.ACL Implementation:

Access Control Lists were applied on R7 to allow only HTTP access to the internal web server and block all other inbound public traffic.

Commands Used:

R7(config)# access-list 100 permit tcp any host 192.168.1.194 eq 80

R7(config)# access-list 100 deny ip any 192.168.1.0 0.0.0.255

R7(config)# access-list 100 permit ip any any

R7(config)# interface g0/0

R7(config-if)# ip access-group 100 in

8.IOT Devices:

IoT devices like smart cameras and temperature sensors were added in the utility subnet and were able to communicate with local servers and management PCs.

📙 Summary and Learning Experience

This project provided an in-depth, hands-on understanding of designing and implementing a scalable enterprise-level network. Through the process of setting up routers, switches, servers, and services such as DNS, DHCP, NAT, and ACLs, I learned how to efficiently manage IP resources and secure network infrastructure.

Using OSPF helped me understand link-state routing benefits, and applying ACLs showed the importance of perimeter security. Configuring multiple web servers, including public and private, tested my understanding of NAT and domain resolution.

Every step required validation, troubleshooting, and logical thinking, which significantly enhanced my practical networking skills and confidence in handling real-world scenarios.
