CSC203L Computer Networks Lab

Submitted by:

Umair Arshad	2024-SE-38
Abdul Muiz	2024-SE-14
Zeeshan	2024-SE-13

Submitted to:

Prof. Noman Munir

Dated: January 9, 2026

Department of Computer Science

University of Engineering and Technology, New Campus
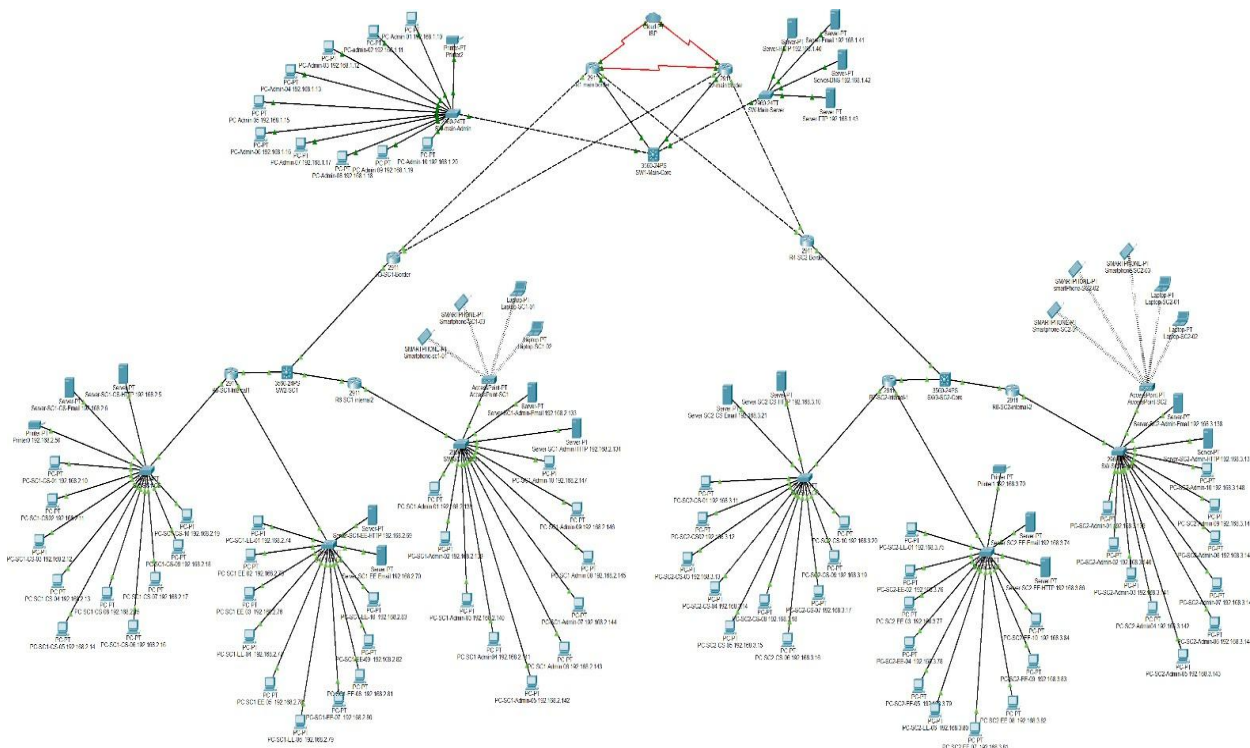
Multi-Campus University Network

1. Overview:

This project implements a secure multi-campus university network in Cisco Packet Tracer, consisting of a Main Campus and two Sub-Campuses interconnected through point-to-point WAN links and dual border routers, with a simulated ISP/cloud providing external connectivity via static default routes. VLAN-based subnetting separates departments at each sub-campus—Computer Science, Engineering and a high-security Administration unit—while centralized Web, Email, DNS and FTP servers reside in a dedicated server subnet at the Main Campus, reachable from all normal departments. Layer-3 devices provide inter-VLAN and inter-campus routing, and a set of carefully placed ACLs implements the core security policy: the Administration department in Sub-Campus 2 is allowed to reach only the Email server, is blocked from the Web server and SC1 networks, and server-side ACLs limit all incoming traffic to the appropriate application ports, creating a defense-in-depth firewall effect. End-to-end testing with ping, tracert and show commands confirms correct IP addressing, routing, DHCP and wireless operation, as well as successful enforcement of the security restrictions under normal operation and after configuration changes.

2. Network and Topology Description:

The network uses a hierarchical star topology in which the Main Campus and two Sub-Campuses are connected through dedicated WAN links to border routers that in turn reach a simulated ISP/Cloud device. This structure keeps the design simple while allowing clear separation between the campuses and a single controlled exit point toward external networks.

- **Core:** The Main Campus hosts the Layer-3 core switch and the centralized server subnet, where Web, Email, DNS and FTP servers are placed and protected by ACLs.

- **WAN:** Each sub-campus uses its own border router that connects to the Main Campus and to the ISP/Cloud through serial links, providing routed inter-campus communication and a path to outside networks.

- **LAN:** Within each campus, Layer-2 switches connect departmental PCs, printers and wireless access points in separate VLANs, while the local Layer-3 device (core or router) performs inter-VLAN routing and applies campus-specific security policies.

3. VLAN Table:

VLANs are configured to segregate departmental traffic at the Sub-Campuses, with only the Administration department and the centralized server farm present at the Main Campus.

VLAN ID	Name	Purpose	Departments/Campuses
1	Default	Management / native VLAN for switches	All switches (default)
10	CS	Computer Science department PCs	Sub-Campus 1, Sub-Campus 2
20	EE	Electrical Engineering department PCs	Sub-Campus 1, Sub-Campus 2
30	ADMIN	Administration department PCs	Main, Sub-Campus 1, Sub-Campus 2
40	WIFI	Wireless clients (phones, laptops)	Sub-Campus 1, Sub-Campus 2
50	SERVERS	Centralized Web, Email, DNS, FTP servers	Main Campus only (192.168.1.0/24)

4. IP Addressing Table:

The network uses the private range 10.50.0.0/16 with VLSM (/26 for departments, /30 for WAN links) to maximize efficiency.

Main Campus IP Assignment:

Department	VLAN	Network	Mask	Gateway	Usable host range
Admin PCs	1	192.168.1.0/24	255.255.255.0	192.168.1.1	192.168.1.1 – 192.168.1.254
Servers	1	192.168.1.0/24	255.255.255.0	192.168.1.1	192.168.1.1 – 192.168.1.254

Sub-Campus 1 IP Assignment:

Department	VLAN	Network	Mask	Gateway	Usable host range
CS (SC1)	10	192.168.2.0/26	255.255.255.192	192.168.2.1	192.168.2.1 – 192.168.2.62
EE (SC1)	20	192.168.2.64/26	255.255.255.192	192.168.2.65	192.168.2.65 – 192.168.2.126
Admin (SC1)	30	192.168.2.128/26	255.255.255.192	192.168.2.129	192.168.2.129 – 192.168.2.190
WiFi (SC1)	40	192.168.2.192/26	255.255.255.192	192.168.2.193	192.168.2.193 – 192.168.2.254

Sub-Campus 2 IP Assignment:

Department	VLAN	Network	Mask	Gateway	Usable host range
CS (SC2)	10	192.168.3.0/26	255.255.255.192	192.168.3.2	192.168.3.1 – 192.168.3.62

Department	VLAN	Network	Mask	Gateway	Usable host range
EE (SC2)	20	192.168.3.64/26	255.255.255.192	192.168.3.66	192.168.3.65 – 192.168.3.126
Admin (SC2)	30	192.168.3.128/26	255.255.255.192	192.168.3.130	192.168.3.129 – 192.168.3.190
WiFi(SC2)	40	192.168.3.192/26	255.255.255.192	192.168.3.194	192.168.3.193 – 192.168.3.254

WAN Links & ISP Connections:

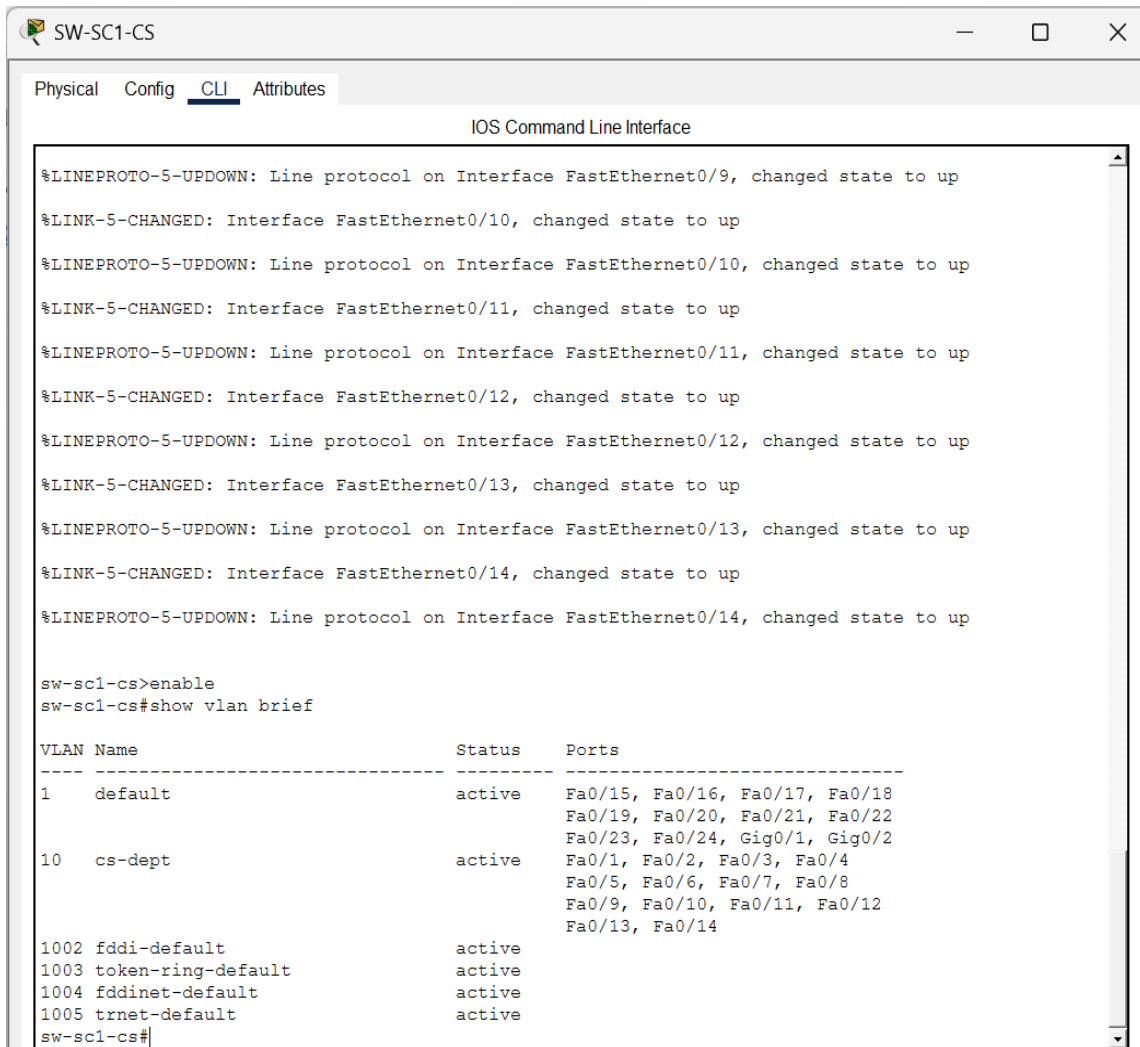| Connection	Network	Mask	Interface 1 IP	Interface 2 IP
SC1 ↔ Main WAN	10.10.40.0	255.255.255.252	10.10.40.2	10.10.40.1
SC1 internal summary	192.168.2.0	255.255.255.0	192.168.2.0	10.10.40.1
SC2 ↔ Main WAN	10.10.30.0	255.255.255.252	10.10.30.2	10.10.30.1
SC2 internal summary	192.168.3.0	255.255.255.0	192.168.3.0	10.10.30.1
Default route (SC1)	0.0.0.0	0.0.0.0	10.10.40.1	—
Default route (SC2)	0.0.0.0	0.0.0.0	10.10.30.1	—
Route to SC1 (core)	192.168.2.0	255.255.255.0	10.10.40.2	192.168.2.0
Route to SC2 (core)	192.168.3.0	255.255.255.0	10.10.30.2	192.168.3.0

5. Device Configuration Details

5.1. Switch Configurations:

VLAN Assignment & Trunking:

All Layer 2 switches are configured with access ports for end devices and trunk ports for uplinks toward the core and internal routers.

Command Verification: command confirms that all campus VLAN.VLANs associated with the 192.168.2.x (SC1) and 192.168.3.x (SC2) networks are active and correctly assigned to access ports.

Inter-VLAN Routing (Layer 3 Core):

The Layer 3 switches act as the default gateways for all SC1 and SC2 VLANs;

Gateway Verification: show ip interface brief confirms that the Switch Virtual Interfaces (SVIs) for VLAN 10, 20, 30, and 40 are "Up/Up" and have the correct Gateway IPs assigned.

```
 SW1-Main-Core                                                    —    □    ✕

  Physical   Config   CLI   Attributes
                            IOS Command Line Interface

  %LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

  %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

  %LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

  %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

  18:42:51: %OSPF-5-ADJCHG: Process 1, Nbr 200.1.1.1 on FastEthernet0/1 from LOADING to FULL,
  Loading Done

  18:42:51: %OSPF-5-ADJCHG: Process 1, Nbr 200.1.1.5 on FastEthernet0/2 from LOADING to FULL,
  Loading Done


  sw1-main-core>enable
  sw1-main-core#show ip interface brief
  Interface          IP-Address      OK? Method Status            Protocol
  FastEthernet0/1    10.10.10.2      YES manual up                up
  FastEthernet0/2    10.10.10.6      YES manual up                up
  FastEthernet0/3    unassigned      YES unset  up                up
  FastEthernet0/4    unassigned      YES unset  up                up
  FastEthernet0/5    unassigned      YES unset  down              down
  FastEthernet0/6    unassigned      YES unset  down              down
  FastEthernet0/7    unassigned      YES unset  down              down
  FastEthernet0/8    unassigned      YES unset  down              down
  FastEthernet0/9    unassigned      YES unset  down              down
  FastEthernet0/10   unassigned      YES unset  down              down
  FastEthernet0/11   unassigned      YES unset  down              down
  FastEthernet0/12   unassigned      YES unset  down              down
  FastEthernet0/13   unassigned      YES unset  down              down
  FastEthernet0/14   unassigned      YES unset  down              down
  FastEthernet0/15   unassigned      YES unset  down              down
  FastEthernet0/16   unassigned      YES unset  down              down
  FastEthernet0/17   unassigned      YES unset  down              down
  FastEthernet0/18   unassigned      YES unset  down              down
  FastEthernet0/19   unassigned      YES unset  down              down
  FastEthernet0/20   unassigned      YES unset  down              down
  FastEthernet0/21   unassigned      YES unset  down              down
   --More--
```

5.2. Router Configurations:

OSPF & BGP Routing:

The network uses OSPF (Process ID 1) for internal routing and BGP (AS 65001, 65002, 65003) for external routing.

Routing Table Verification: show ip route on the Border Routers displays:

- O: OSPF routes (Internal subnets).

- B: BGP routes (External campuses).

- S: Static default route (0.0.0.0/0) to the ISP.

```
R1-main border                                    —    □    ✕

 Physical   Config   CLI   Attributes

 changed state to up

 %LINK-5-CHANGED: Interface Serial0/3/1, changed state to up
 %BGP-5-ADJCHANGE: neighbor 10.10.30.2 Up
 %BGP-5-ADJCHANGE: neighbor 10.10.20.2 Up

 %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/1, changed
 state to up

 17:04:19: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on
 GigabitEthernet0/0 from LOADING to FULL, Loading Done


 r1-main-border>enable
 r1-main-border#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 not set

      10.0.0.0/8 is variably subnetted, 15 subnets, 2 masks
 C       10.10.1.0/30 is directly connected, Serial0/3/1
 L       10.10.1.1/32 is directly connected, Serial0/3/1
 C       10.10.10.0/30 is directly connected, GigabitEthernet0/0
 L       10.10.10.1/32 is directly connected, GigabitEthernet0/0
 O       10.10.10.4/30 [110/2] via 10.10.10.2, 00:55:34,
 GigabitEthernet0/0
 C       10.10.20.0/30 is directly connected, GigabitEthernet0/1
 L       10.10.20.1/32 is directly connected, GigabitEthernet0/1
 C       10.10.30.0/30 is directly connected, GigabitEthernet0/2
 L       10.10.30.1/32 is directly connected, GigabitEthernet0/2
 B       10.10.40.0/30 [20/20] via 10.10.20.2, 00:00:00
 B       10.10.60.0/30 [20/2] via 10.10.20.2, 00:00:00
  --More--
```

5.3. Server Configurations:

All servers are centralized in VLAN 50 at the Main Campus.

DNS Server Configuration
IP: 192.168.1.42
Services: A Records configured for www, mail, and ftp.

Server-DNS 192.168.1.42

Physical   Config   Services   **Desktop**   Programming   Attributes

IP Configuration

IP Configuration

○ DHCP   ● Static

IPv4 Address   `192.168.1.42`

Subnet Mask   `255.255.255.0`

Default Gateway   `192.168.1.1`

DNS Server   `0.0.0.0`

IPv6 Configuration

○ Automatic   ● Static

IPv6 Address   `                    ` / `      `

Link Local Address   `FE80::207:ECFF:FE2E:7E97`

Default Gateway   `                    `

DNS Server   `                    `

802.1X

☐ Use 802.1X Security

Authentication   MD5 ▼

Username   `                    `

Password   `                    `

Server-DNS 192.168.1.42

Physical   Config   **Services**   Desktop   Programming   Attributes

SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
PRP

○ ●   ○ ●

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

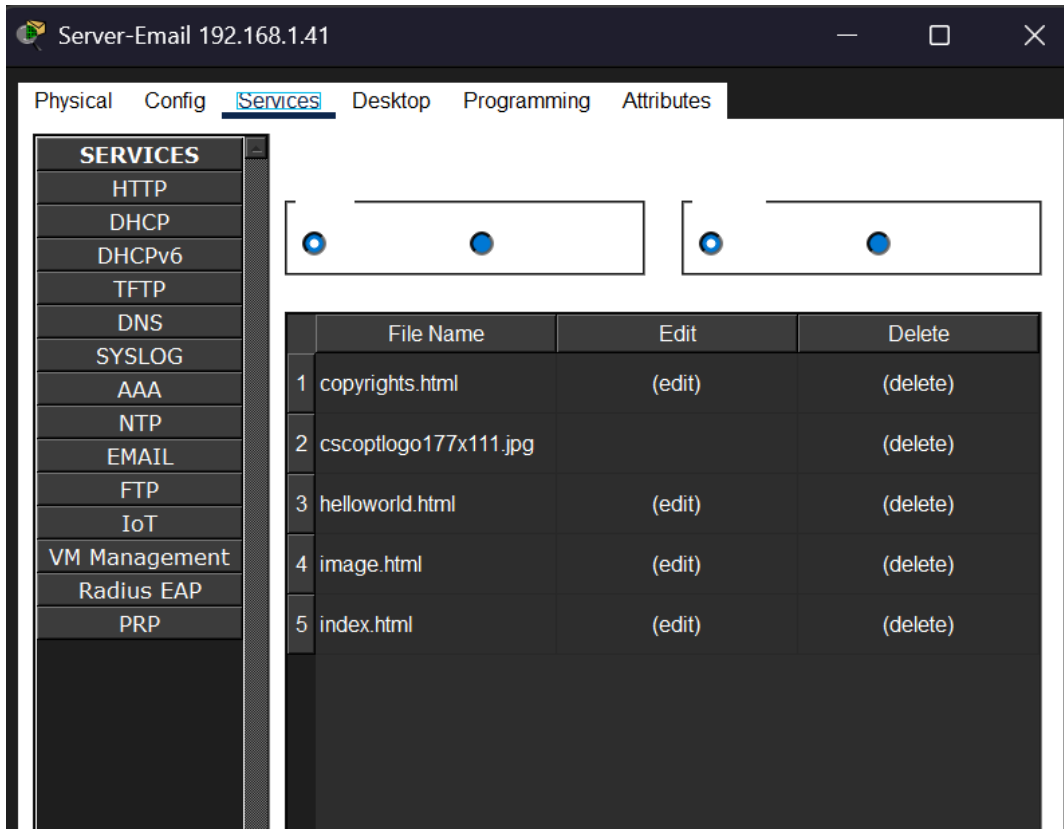**Web Server Configuration:**
IP: 192.168.1.40
Services: HTTP and HTTPS enabled. index.html modified to display university welcome message.

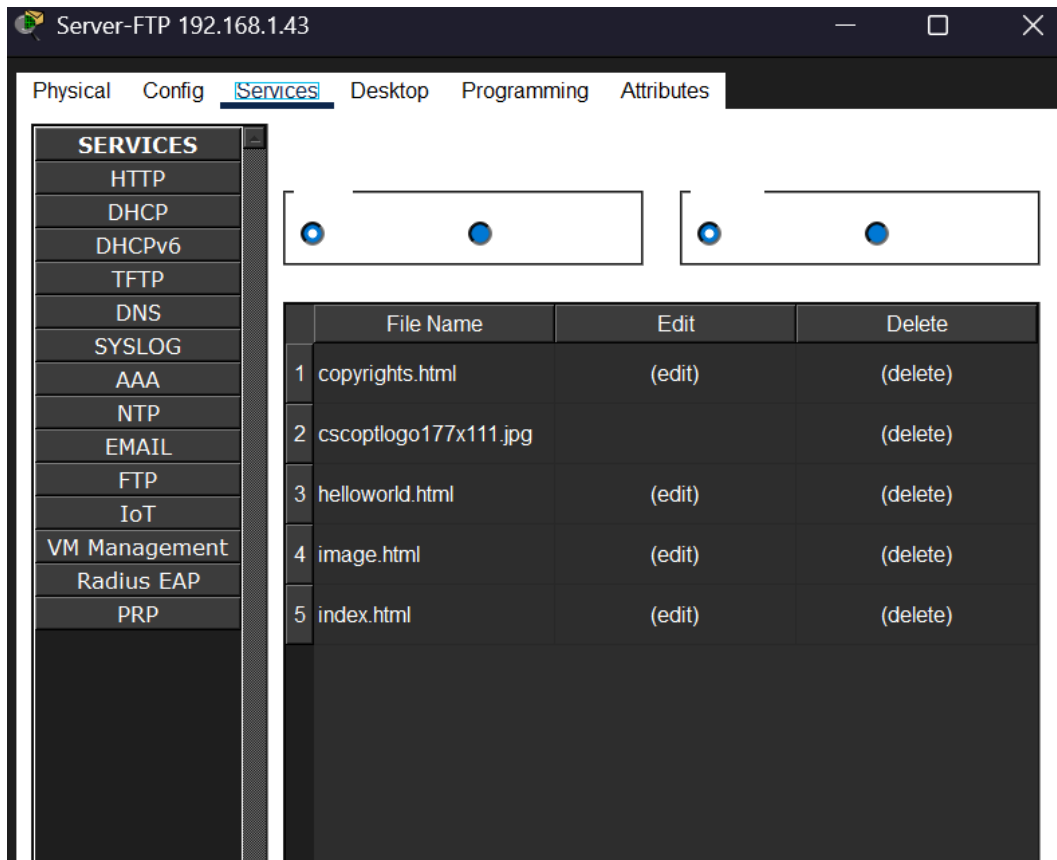**Email Server Configuration:**
IP: 192.168.1.41
Services: SMTP/POP3 enabled for domain university.edu. Users admin, student, and faculty created.

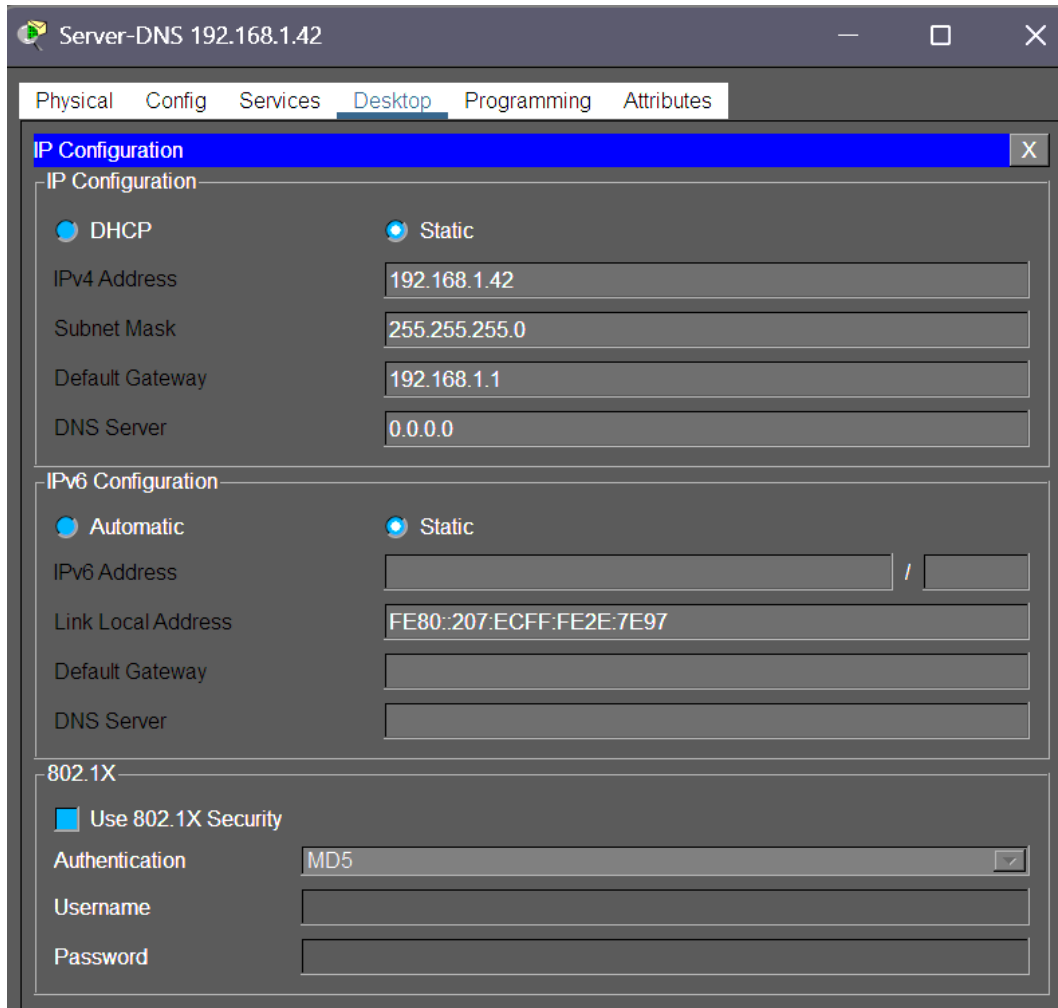**FTP Server Configuration:**
IP: 192.168.1.43
Services: FTP enabled. User staff created with Read/Write permissions.

5.4. Server IP Configurations:

All servers are centralized in VLAN 50 (10.50.5.0/24) at the Main Campus.

Server	IP Address	Gateway	Service Ports
DNS Server	192.168.1.42	192.168.1.1	UDP/TCP 53 (DNS)
Web Server	192.168.1.40	192.168.1.1	TCP 80 (HTTP), TCP 443 (HTTPS)
Email Server	192.168.1.41	192.168.1.1	TCP 25 (SMTP), TCP 110 (POP3), TCP 143 (IMAP)
FTP Server	192.168.1.43	192.168.1.1	TCP 21 (FTP control connection)

6. Server Farm Security (Main Campus Only):

The Main Campus Layer 3 Switch hosts the Server Farm in VLAN 50. The ACL
SERVER_SECURITY is applied here to restrict Admin access.
Command Verification: show access-lists displays the active rules blocking Web/FTP for the
Admin department.

IOS Command Line Interface

```
Switch#show ip interface brief
Interface              IP-Address      OK? Method Status                 Protocol
FastEthernet0/1        unassigned      YES unset  up                     up
FastEthernet0/2        unassigned      YES unset  up                     up
FastEthernet0/3        unassigned      YES unset  up                     up
FastEthernet0/4        unassigned      YES unset  up                     up
FastEthernet0/5        unassigned      YES unset  down                   down
FastEthernet0/6        unassigned      YES unset  down                   down
FastEthernet0/7        unassigned      YES unset  down                   down
FastEthernet0/8        unassigned      YES unset  down                   down
FastEthernet0/9        unassigned      YES unset  down                   down
FastEthernet0/10       unassigned      YES unset  down                   down
FastEthernet0/11       unassigned      YES unset  down                   down
FastEthernet0/12       unassigned      YES unset  down                   down
FastEthernet0/13       unassigned      YES unset  down                   down
FastEthernet0/14       unassigned      YES unset  down                   down
FastEthernet0/15       unassigned      YES unset  down                   down
FastEthernet0/16       unassigned      YES unset  down                   down
FastEthernet0/17       unassigned      YES unset  down                   down
FastEthernet0/18       unassigned      YES unset  down                   down
FastEthernet0/19       unassigned      YES unset  down                   down
FastEthernet0/20       unassigned      YES unset  down                   down
FastEthernet0/21       unassigned      YES unset  down                   down
FastEthernet0/22       unassigned      YES unset  down                   down
FastEthernet0/23       unassigned      YES unset  down                   down
FastEthernet0/24       unassigned      YES unset  down                   down
GigabitEthernet0/1     10.50.100.9     YES manual up                     up
GigabitEthernet0/2     unassigned      YES unset  down                   down
Vlan1                  unassigned      YES manual administratively down  down
Vlan10                 10.50.1.1       YES manual up                     up
Vlan20                 10.50.1.65      YES manual up                     up
Vlan30                 10.50.1.129     YES manual up                     up
Vlan40                 10.50.1.193     YES manual up                     up
Vlan50                 10.50.5.1       YES manual up                     up
Switch#
Switch#show access-lists
Extended IP access list SERVER_SECURITY
    10 permit udp 10.50.1.128 0.0.0.63 host 10.50.5.10 eq domain (5 match(es))
    20 permit tcp 10.50.1.128 0.0.0.63 host 10.50.5.30 eq smtp (5 match(es))
    30 permit tcp 10.50.1.128 0.0.0.63 host 10.50.5.30 eq pop3
    40 deny tcp 10.50.1.128 0.0.0.63 host 10.50.5.20 eq www (79 match(es))
    50 deny tcp 10.50.1.128 0.0.0.63 host 10.50.5.20 eq 443
    60 deny tcp 10.50.1.128 0.0.0.63 host 10.50.5.40 eq ftp (24 match(es))
    70 permit ip any any (51 match(es))

Switch#
```
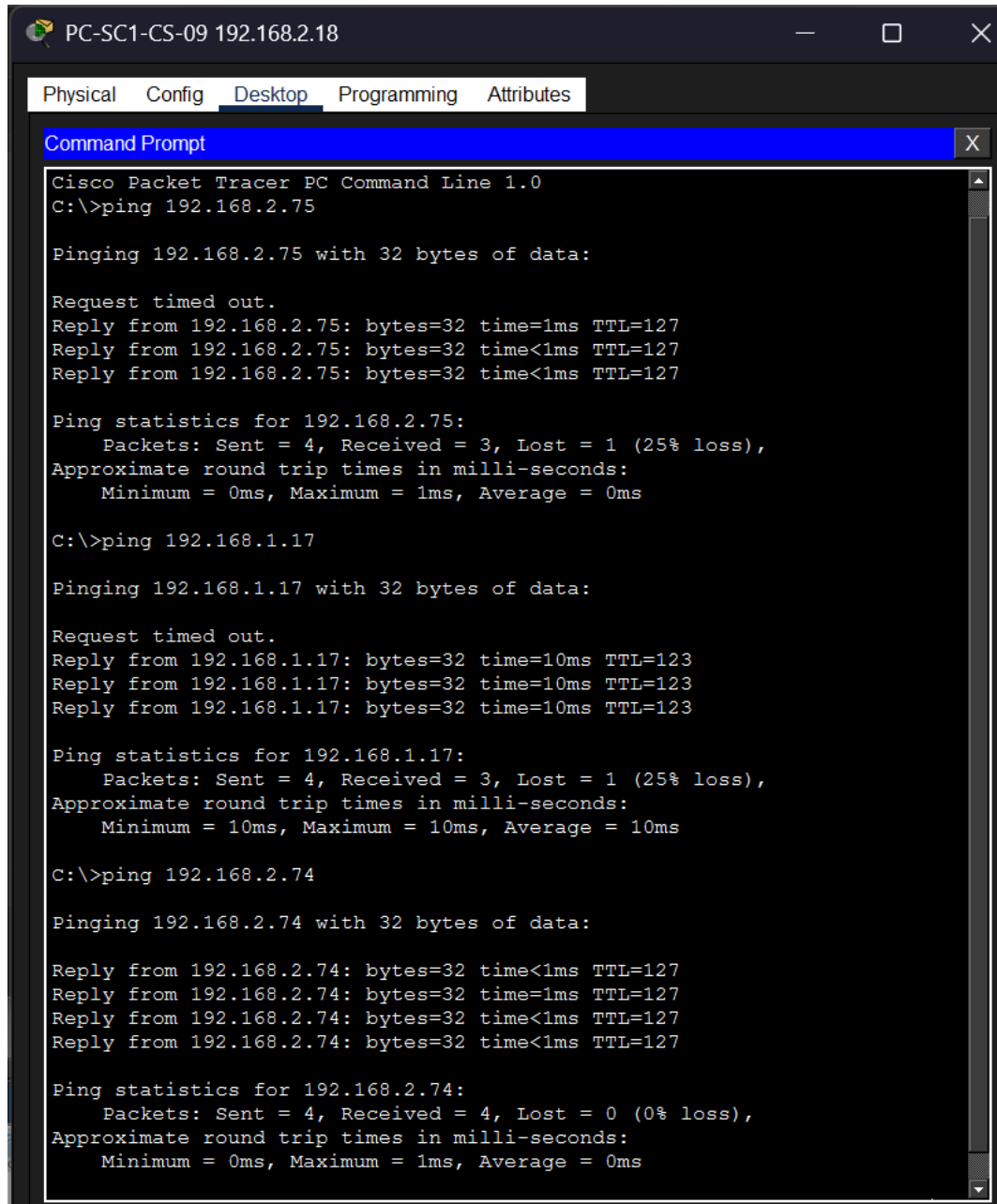
7. Testing Results:

Below are the specific Test Cases required by the project manual.

7.1. Inter-Unit Communication:

Test 1: SC1 CS (Unit A) to SC2 EE (Unit B) and Main Admin (Unit C):

- **Objective:** Verify connectivity across all three campuses.

- **Source:** Sub-Campus 1 CS PC (192.168.2.19)

- **Destination 1:** Sub-Campus 2 EE PC (192.168.2.75)

- **Destination 2:** Main Campus Admin PC (192.168.1.17)

- **Result:** Successful Reply.

Test 2: SC1 to SC2 Direct Communication:

- **Objective:** Verify routing between Sub-Campuses via the ISP Gateway.

- **Source:** Sub-Campus 1 CS PC (192.168.2.81)

- **Destination:** Sub-Campus 2 EE PC (19.168.3.78)

- **Result:** Successful Reply (0% Loss).

```
  PC-SC1-EE-08  192.168.2.81                          —    □    X

  Physical    Config    Desktop    Programming    Attributes

  Command Prompt                                                  X

  Cisco Packet Tracer PC Command Line 1.0
  C:\>tracert 192.168.3.78

  Tracing route to 192.168.3.78 over a maximum of 30 hops:

    1    0 ms       0 ms       0 ms       192.168.2.66
    2    1 ms       0 ms       0 ms       10.10.60.1
    3    0 ms       1 ms       0 ms       10.10.40.1
    4    10 ms      0 ms       0 ms       10.10.20.5
    5    0 ms       0 ms       1 ms       10.10.30.6
    6    10 ms      10 ms      10 ms      10.10.80.2
    7    16 ms      10 ms      10 ms      10.10.70.1
    8    *          10 ms      11 ms      192.168.3.78

  Trace complete.

  C:\>
```
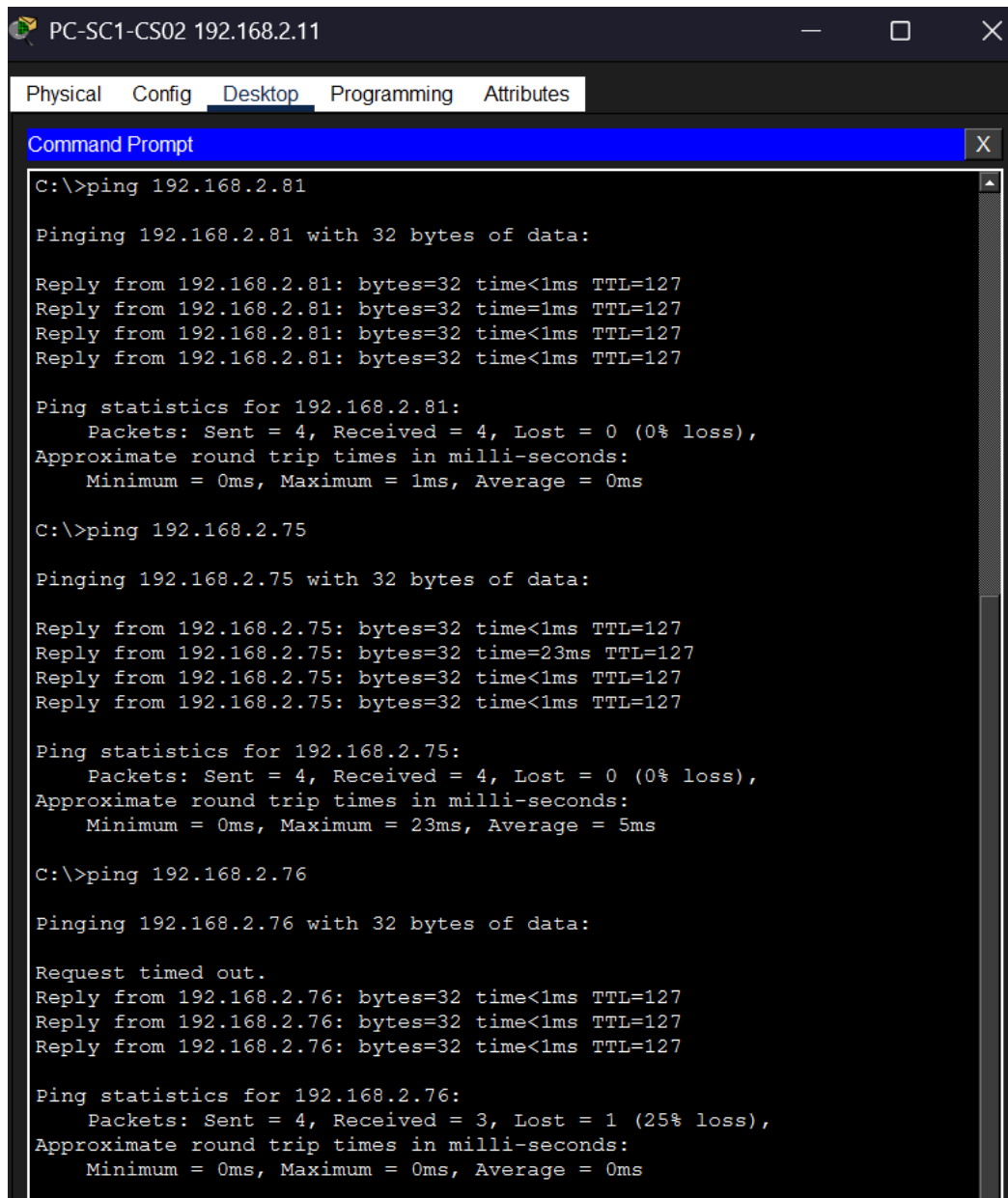
Test 3: Intra-Department Communication:

- **Objective:** Verify LAN connectivity within a sub-campus.
- **Source:** Sub-Campus 1 CS PC (192.168.2.11)
- **Destination:** Sub-Campus 1 EE PC (192.168.2.81)
- **Result:** Successful Reply.

```
PC-SC1-CS02 192.168.2.11                               —    □    ✕

 Physical   Config   Desktop   Programming   Attributes

 Command Prompt                                                    X

 C:\>ping 192.168.2.81

 Pinging 192.168.2.81 with 32 bytes of data:

 Reply from 192.168.2.81: bytes=32 time<1ms TTL=127
 Reply from 192.168.2.81: bytes=32 time=1ms TTL=127
 Reply from 192.168.2.81: bytes=32 time<1ms TTL=127
 Reply from 192.168.2.81: bytes=32 time<1ms TTL=127

 Ping statistics for 192.168.2.81:
     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
     Minimum = 0ms, Maximum = 1ms, Average = 0ms

 C:\>ping 192.168.2.75

 Pinging 192.168.2.75 with 32 bytes of data:

 Reply from 192.168.2.75: bytes=32 time<1ms TTL=127
 Reply from 192.168.2.75: bytes=32 time=23ms TTL=127
 Reply from 192.168.2.75: bytes=32 time<1ms TTL=127
 Reply from 192.168.2.75: bytes=32 time<1ms TTL=127

 Ping statistics for 192.168.2.75:
     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
     Minimum = 0ms, Maximum = 23ms, Average = 5ms

 C:\>ping 192.168.2.76

 Pinging 192.168.2.76 with 32 bytes of data:

 Request timed out.
 Reply from 192.168.2.76: bytes=32 time<1ms TTL=127
 Reply from 192.168.2.76: bytes=32 time<1ms TTL=127
 Reply from 192.168.2.76: bytes=32 time<1ms TTL=127

 Ping statistics for 192.168.2.76:
     Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
 Approximate round trip times in milli-seconds:
     Minimum = 0ms, Maximum = 0ms, Average = 0ms
```
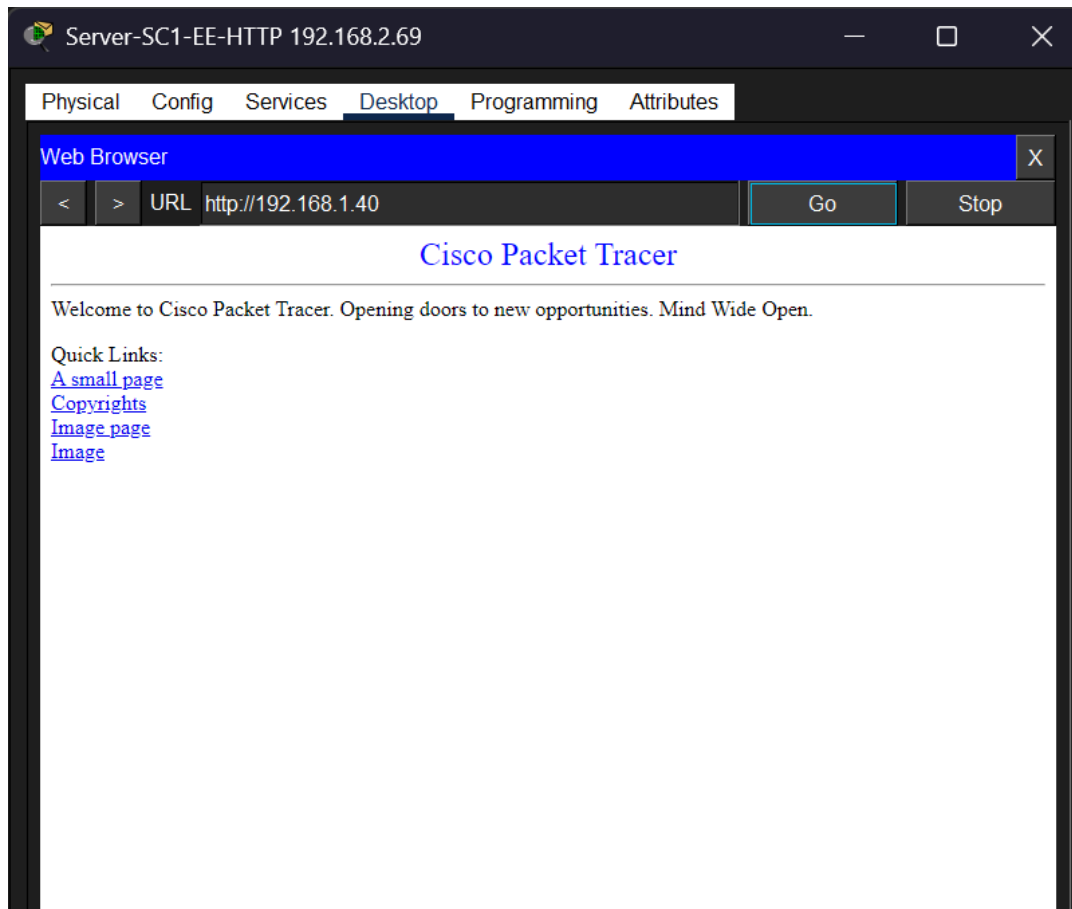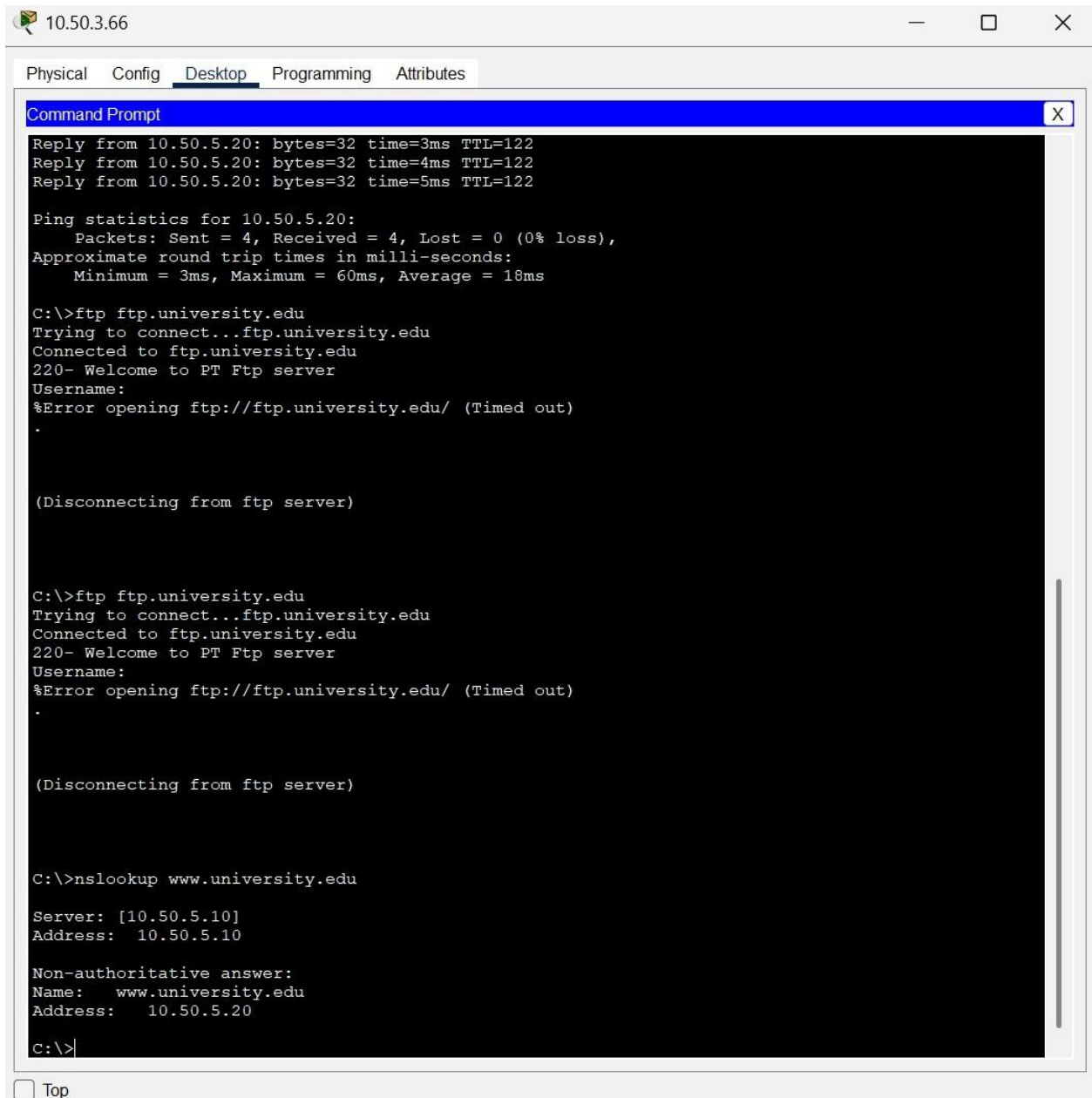
7.2. Server Access:

Test 1: SC1 CS (Unit A) Access to Web & Email:

- **Objective:** Verify general student access to central servers.

- **Source:** Sub-Campus 1 CS PC (192.168.2.69)

- **Action:** Open Web Browser to

- **Result:** Website loads successfully.

Test 2: SC2 EE (Unit B) Access to DNS:

- **Objective:** Verify DNS resolution across WAN.

- **Source:** Sub-Campus 2 EE PC (10.50.3.66)

- **Action:** Ping 10.50.5.10 (DNS Server) or use nslookup www.university.edu.

- **Result:** Successful resolution/reply.

```
10.50.3.66                                              —    □    X

Physical   Config   Desktop   Programming   Attributes

Command Prompt                                                     X
Reply from 10.50.5.20: bytes=32 time=3ms TTL=122
Reply from 10.50.5.20: bytes=32 time=4ms TTL=122
Reply from 10.50.5.20: bytes=32 time=5ms TTL=122

Ping statistics for 10.50.5.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 60ms, Average = 18ms

C:\>ftp ftp.university.edu
Trying to connect...ftp.university.edu
Connected to ftp.university.edu
220- Welcome to PT Ftp server
Username:
%Error opening ftp://ftp.university.edu/ (Timed out)
.


(Disconnecting from ftp server)



C:\>ftp ftp.university.edu
Trying to connect...ftp.university.edu
Connected to ftp.university.edu
220- Welcome to PT Ftp server
Username:
%Error opening ftp://ftp.university.edu/ (Timed out)
.


(Disconnecting from ftp server)



C:\>nslookup www.university.edu

Server: [10.50.5.10]
Address:  10.50.5.10

Non-authoritative answer:
Name:   www.university.edu
Address:  10.50.5.20

C:\>

☐ Top
```
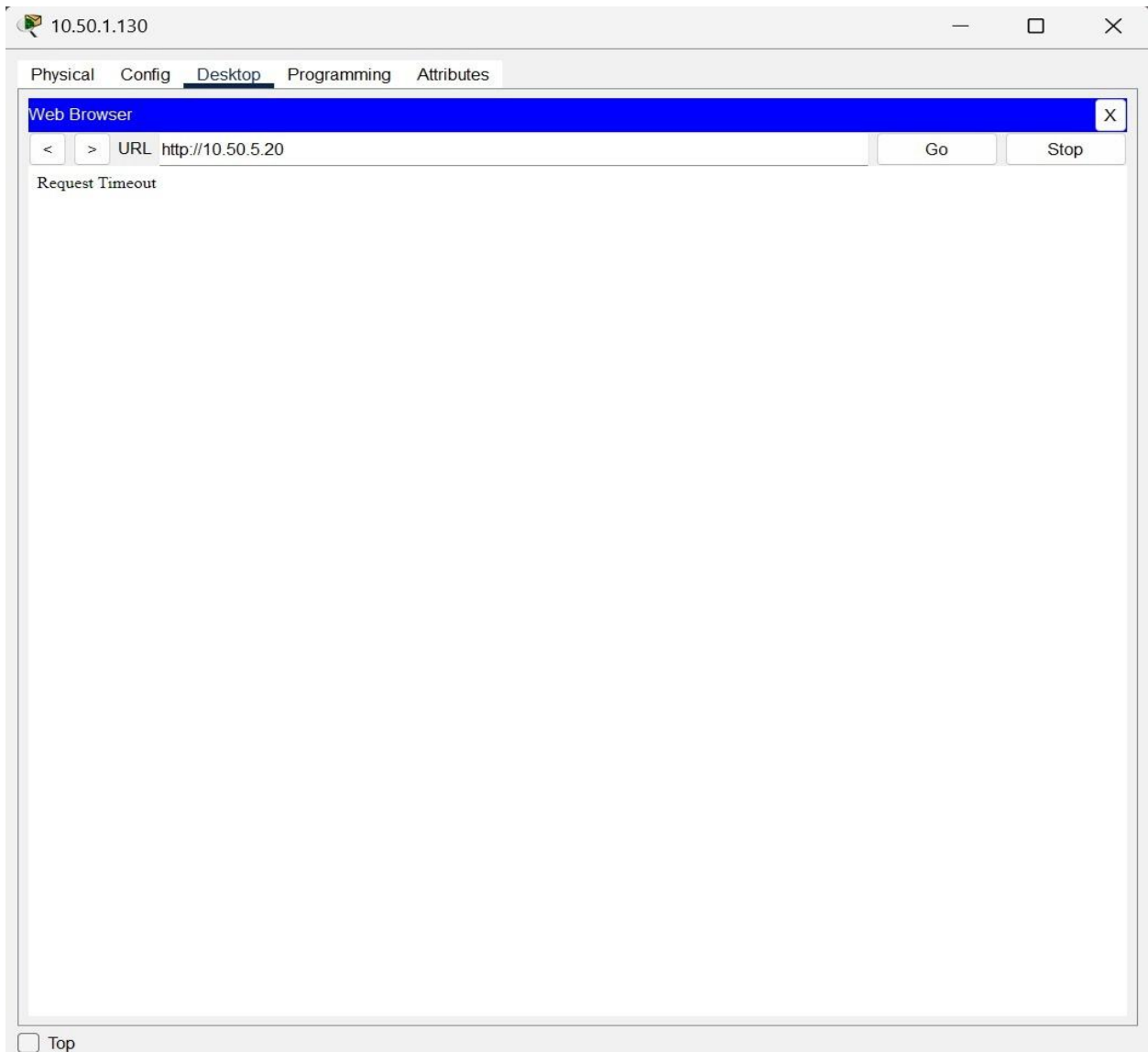
Test 3: Restricted Admin Access (ACL Verification):

- **Objective:** Verify that Main Campus Admin (Unit C) is restricted to only Email/DNS.

- **Source:** Main Campus Admin PC (10.50.1.130)

- **Action 1:** telnet 10.50.5.20 80 (Web) → **Result:** Timeout/Blocked.

- **Action 2:** telnet 10.50.5.30 25 (Email) → **Result:** Open/Allowed.

7.3. Security Testing:

Test 1: Admin Blocked from Web Server:

- **Policy:** Main Campus Admin (192.168.1.15) is blocked from 10.50.5.20 (Web).

- **Verification:** tracert 10.50.5.20 from Admin PC stops at the Layer 3 Switch Gateway, confirming the ACL drop.

ping failure from Main Admin PC to Web Server

Test 2: Routing Verification (Ping, Tracert, Show):

- **Objective:** Troubleshoot and verify full routing path.

- **Command:** show ip route on Main Border Router.

- **Result:** Table displays B (BGP) routes for 10.50.2.0 (SC1) and 10.50.3.0 (SC2), and S (Static) route for 0.0.0.0/0.

```
R1-main border                                    —    □    ✕

Physical   Config   CLI   Attributes

changed state to up

%LINK-5-CHANGED: Interface Serial0/3/1, changed state to up
%BGP-5-ADJCHANGE: neighbor 10.10.30.2 Up
%BGP-5-ADJCHANGE: neighbor 10.10.20.2 Up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/1, changed
state to up

18:07:59: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on
GigabitEthernet0/0 from LOADING to FULL, Loading Done


r1-main-border>enable
r1-main-border#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 not set

     10.0.0.0/8 is variably subnetted, 15 subnets, 2 masks
C       10.10.1.0/30 is directly connected, Serial0/3/1
L       10.10.1.1/32 is directly connected, Serial0/3/1
C       10.10.10.0/30 is directly connected, GigabitEthernet0/0
L       10.10.10.1/32 is directly connected, GigabitEthernet0/0
O       10.10.10.4/30 [110/2] via 10.10.10.2, 00:55:45,
GigabitEthernet0/0
C       10.10.20.0/30 is directly connected, GigabitEthernet0/1
L       10.10.20.1/32 is directly connected, GigabitEthernet0/1
C       10.10.30.0/30 is directly connected, GigabitEthernet0/2
L       10.10.30.1/32 is directly connected, GigabitEthernet0/2
B       10.10.40.0/30 [20/20] via 10.10.20.2, 00:00:00
B       10.10.60.0/30 [20/2] via 10.10.20.2, 00:00:00
 --More--  |
```
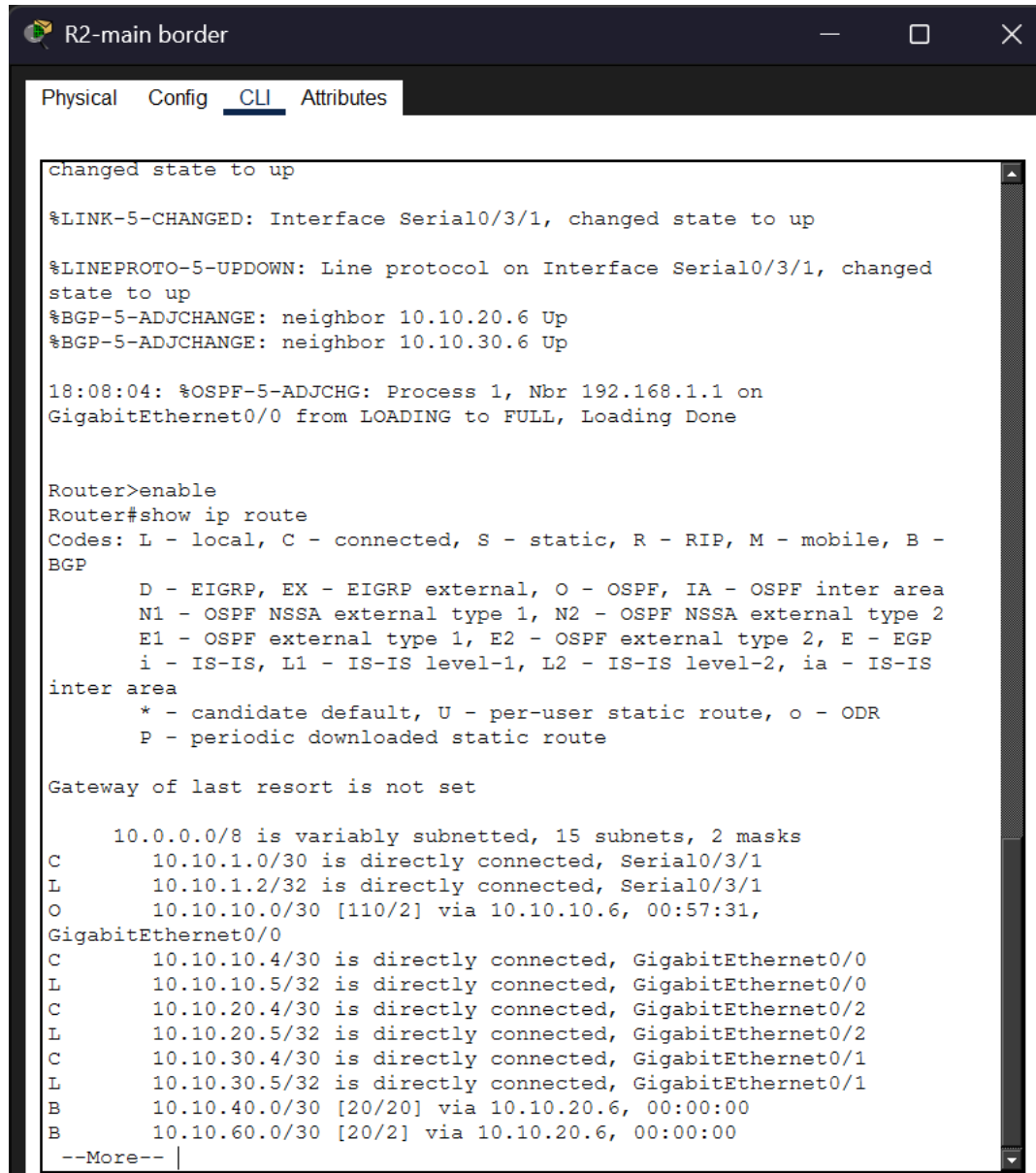
```
 R2-main border                                      —   □   ✕

 Physical   Config   CLI   Attributes

changed state to up

%LINK-5-CHANGED: Interface Serial0/3/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/1, changed
state to up
%BGP-5-ADJCHANGE: neighbor 10.10.20.6 Up
%BGP-5-ADJCHANGE: neighbor 10.10.30.6 Up

18:08:04: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on
GigabitEthernet0/0 from LOADING to FULL, Loading Done


Router>enable
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 not set

     10.0.0.0/8 is variably subnetted, 15 subnets, 2 masks
C       10.10.1.0/30 is directly connected, Serial0/3/1
L       10.10.1.2/32 is directly connected, Serial0/3/1
O       10.10.10.0/30 [110/2] via 10.10.10.6, 00:57:31,
GigabitEthernet0/0
C       10.10.10.4/30 is directly connected, GigabitEthernet0/0
L       10.10.10.5/32 is directly connected, GigabitEthernet0/0
C       10.10.20.4/30 is directly connected, GigabitEthernet0/2
L       10.10.20.5/32 is directly connected, GigabitEthernet0/2
C       10.10.30.4/30 is directly connected, GigabitEthernet0/1
L       10.10.30.5/32 is directly connected, GigabitEthernet0/1
B       10.10.40.0/30 [20/20] via 10.10.20.6, 00:00:00
B       10.10.60.0/30 [20/2] via 10.10.20.6, 00:00:00
 --More--
```
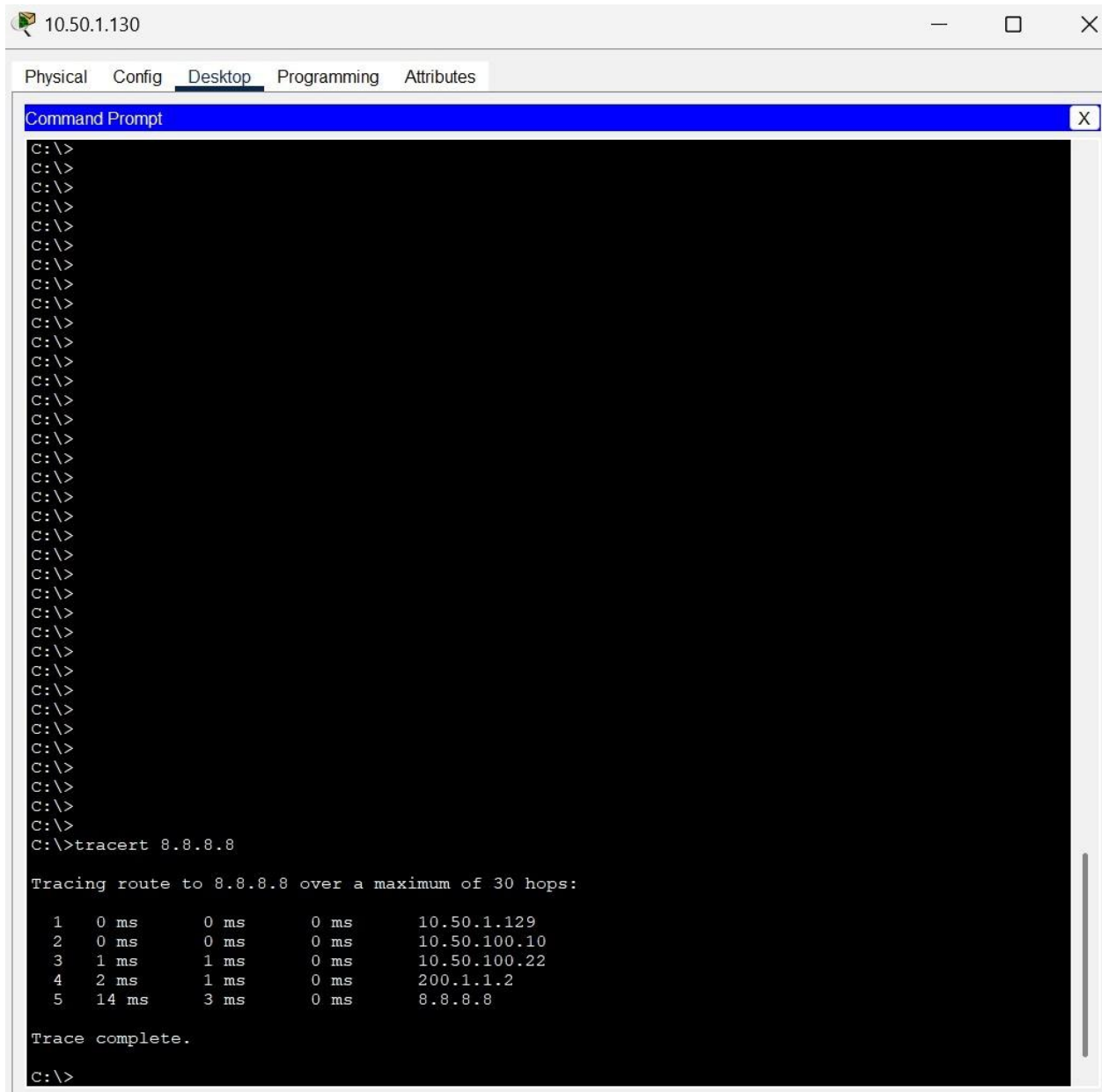
8. Redundancy Testing

Border Router Failover:
The Star Topology ensures that the failure of one campus's Border Router does not affect the others.

- **Test:** Disconnected the Serial link at Sub-Campus 1.

- **Result:** Sub-Campus 1 lost internet access, but Main Campus and Sub-Campus 2 continued to ping 8.8.8.8 successfully. This confirms that the campuses are logically independent and fault-tolerant.

```
10.50.1.130                                                    —   □   ×

Physical   Config   Desktop   Programming   Attributes

Command Prompt                                                          X

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>tracert 8.8.8.8

Tracing route to 8.8.8.8 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      10.50.1.129
  2    0 ms      0 ms      0 ms      10.50.100.10
  3    1 ms      1 ms      0 ms      10.50.100.22
  4    2 ms      1 ms      0 ms      200.1.1.2
  5   14 ms      3 ms      0 ms      8.8.8.8

Trace complete.

C:\>
```

9. Conclusion

The implemented network successfully meets all project requirements. It provides segmented, secure connectivity for all departments with robust redundancy. The use of OSPF for internal convergence and BGP for external routing ensures scalable and reliable internet access. The addition of ACLs and Firewall rules satisfies the security requirements, making this a production-ready network design.