

Network Engineering Capstone Functionality Report Packet Tracer

Introduction

Provide a functionality report detailing the 10 test-case scenarios used to verify the utility of your network project. Seven of the test-case scenarios must be from the provided predefined list, with the remaining three test cases created by you. The functionality report should be written so that a networking peer could replicate the steps for a successful test of your networking solution.

Student Name	Luis Andrade
WGU Student ID	010515598
WGU Student Email	land593@wgu.edu



Test Case #1: Device Discovery and Reachability

Your network solution must include multiple network segments with access controls that allow traffic from a device on one network to access the resources of a device on another network. Similarly, there must be devices on one network that cannot access resources on a different network.

Functionality

*Describe the **functionality** of the test case in relation to your network project. Identify the relevant tools (devices, subnets, etc.) used in this test case and their specific interactions.*

The TrueCover Insurance Solutions organization has both internal and external networks. The internal network consists of end devices segmented into their own VLANs. Some devices use static IP addresses, while others obtain IP addresses via DHCP.

Internal Networks:

IT VLAN 10 – 192.168.0.16/29
SALES VLAN 20 – 192.168.0.24/29
GUEST VLAN 30 – 192.168.0.32/29

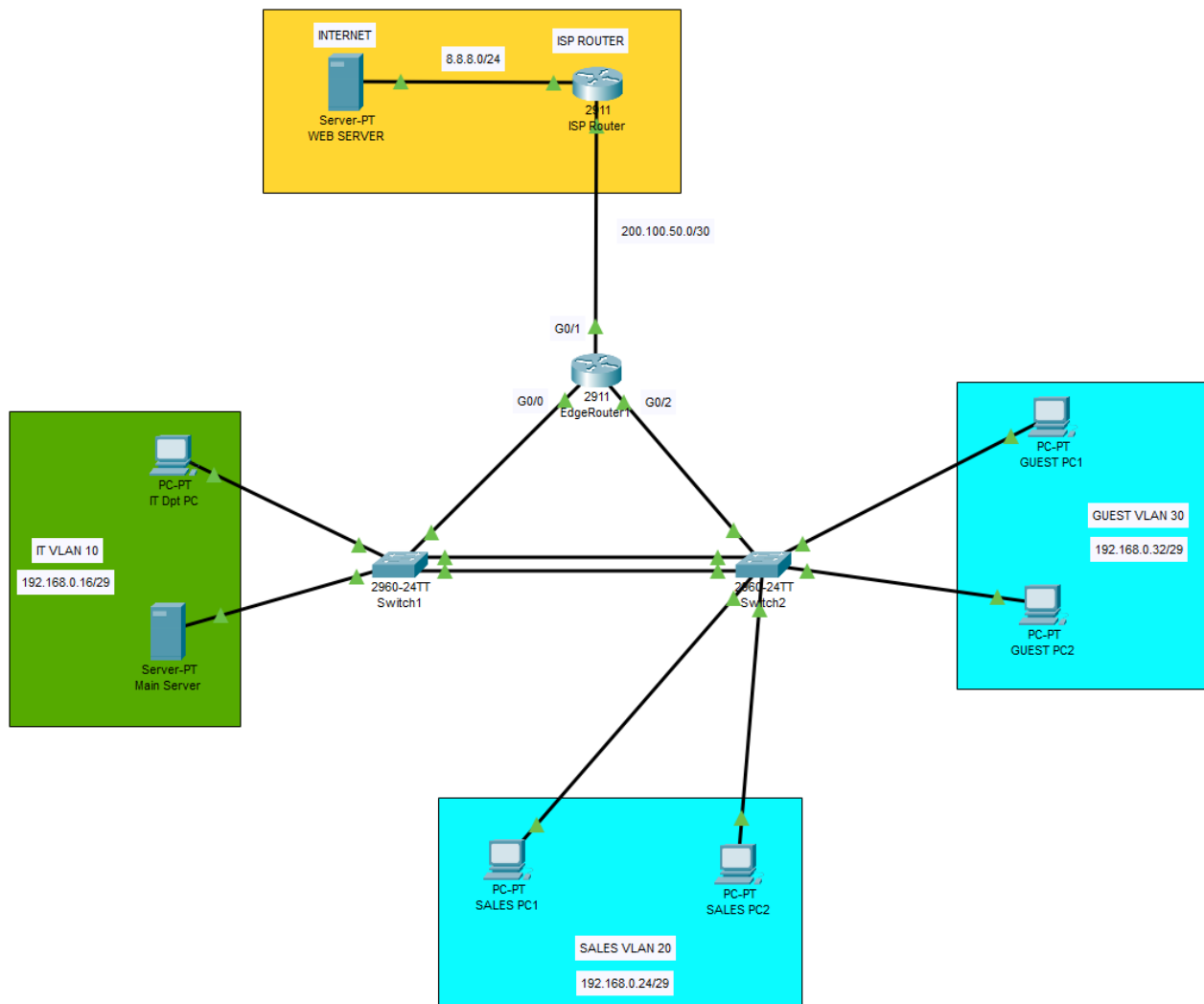
External Networks:

EdgeRouter1 <-> ISP Router – 200.100.50.0/30
ISP Router <-> Internet – 8.8.8.0/24

Network Diagram or Segment

*Provide a **network diagram or segment** visualizing the topology and devices used in this test case.*





Testing Method

Summarize the **testing method** used to verify functionality of the network project within the virtual lab environment, including any metrics of success.

The network includes multiple segments protected by access control lists (ACLs) that permit or deny traffic according to the organization's requirements. The following testing method demonstrates how the IT Department PC, located in IT VLAN 10 with IP address 192.168.0.18, can reach the Internet by initiating a ping or TCP connection. The ACL allows return traffic only if the connection is established. Additionally, the same ACL denies any new connection initiated from the Internet toward IT VLAN 10. This ACL is configured on interface G0/1 of EdgeRouter1, which faces the ISP router.

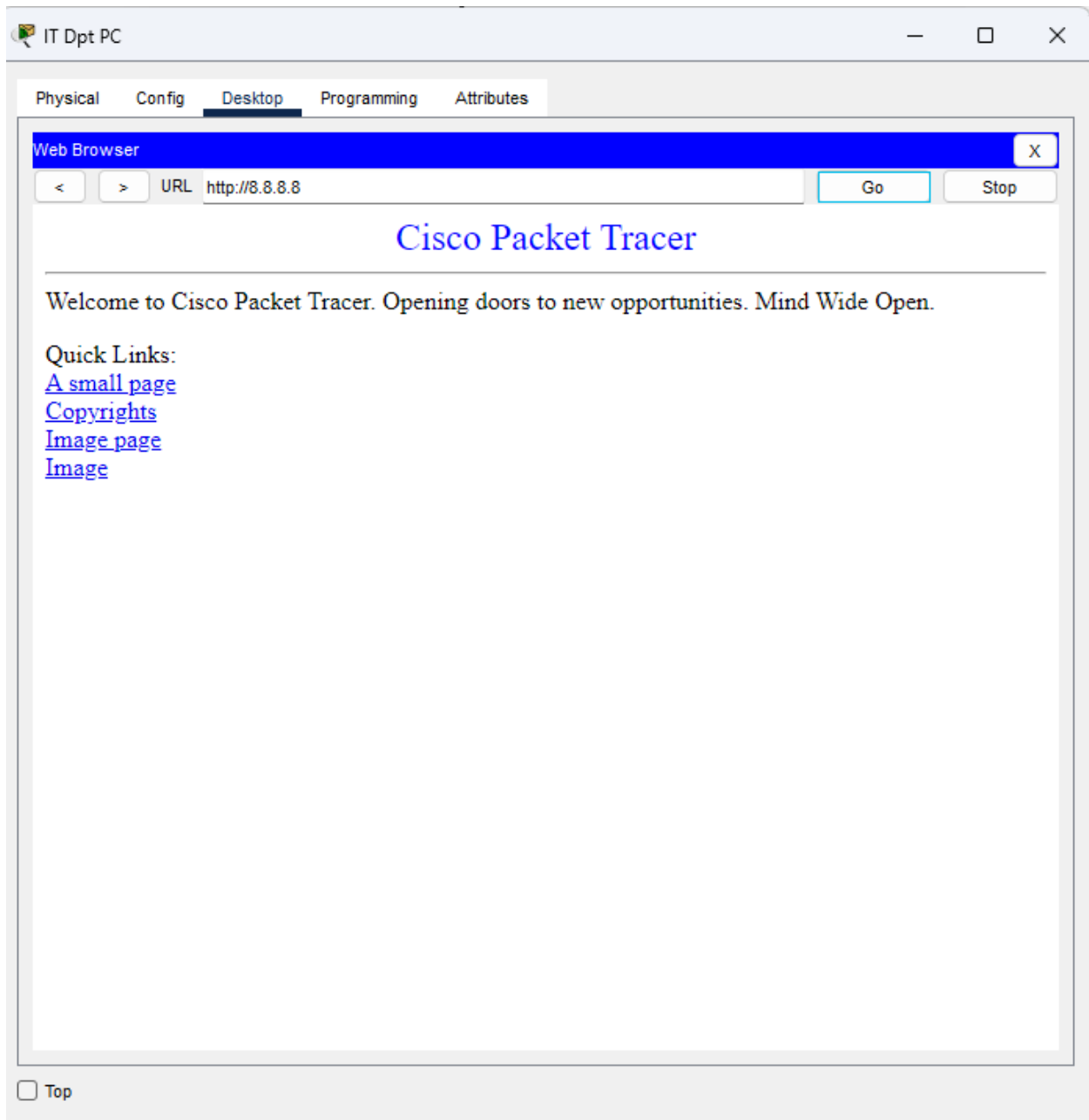


Process List

Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.

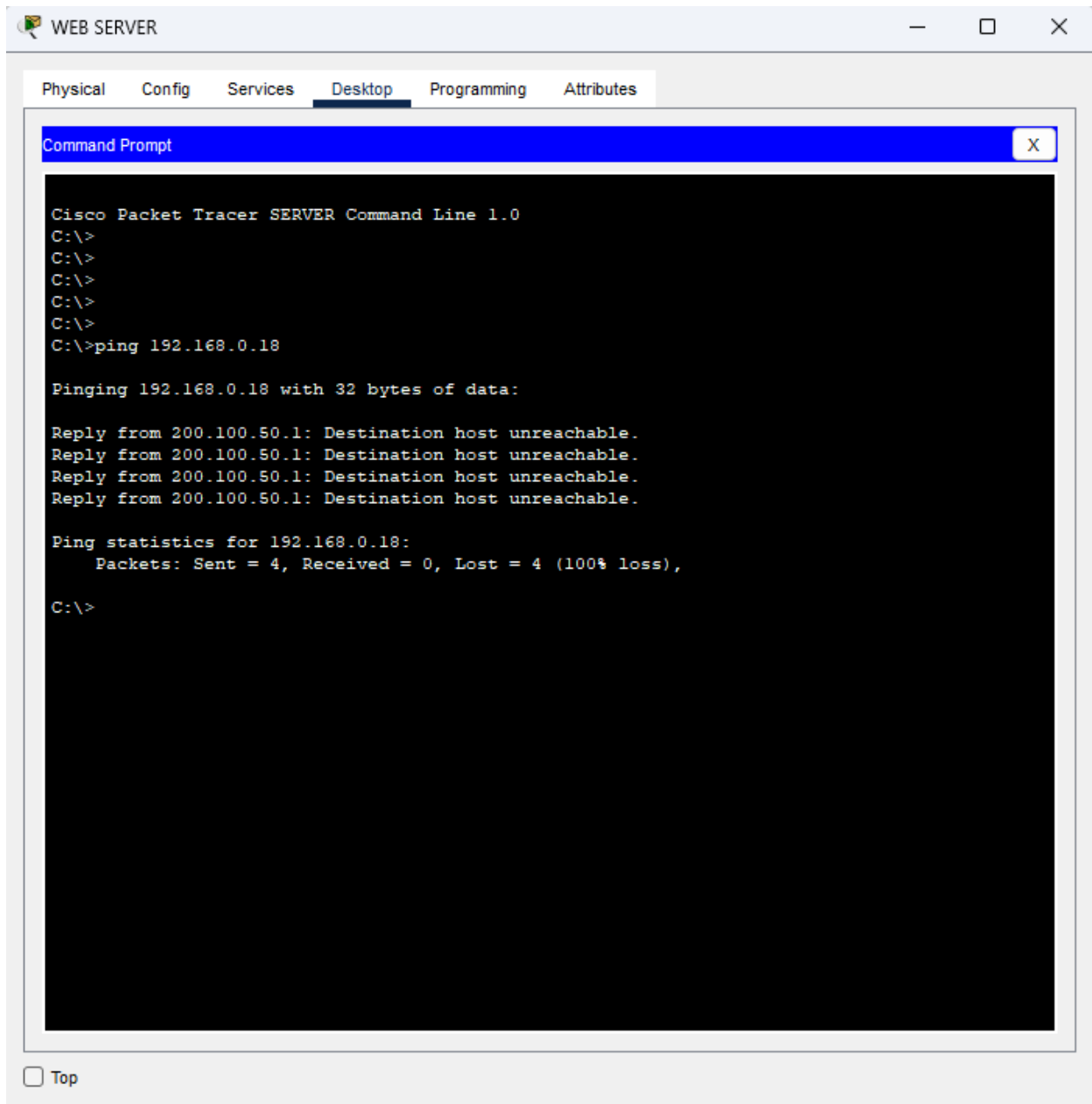
Permit ACL Statement:

1. Access the IT Dpt PC on VLAN 10.
2. Open the command prompt.
3. Ping the web server with IP address 8.8.8.8.
4. Confirm that replies are received from 8.8.8.8.

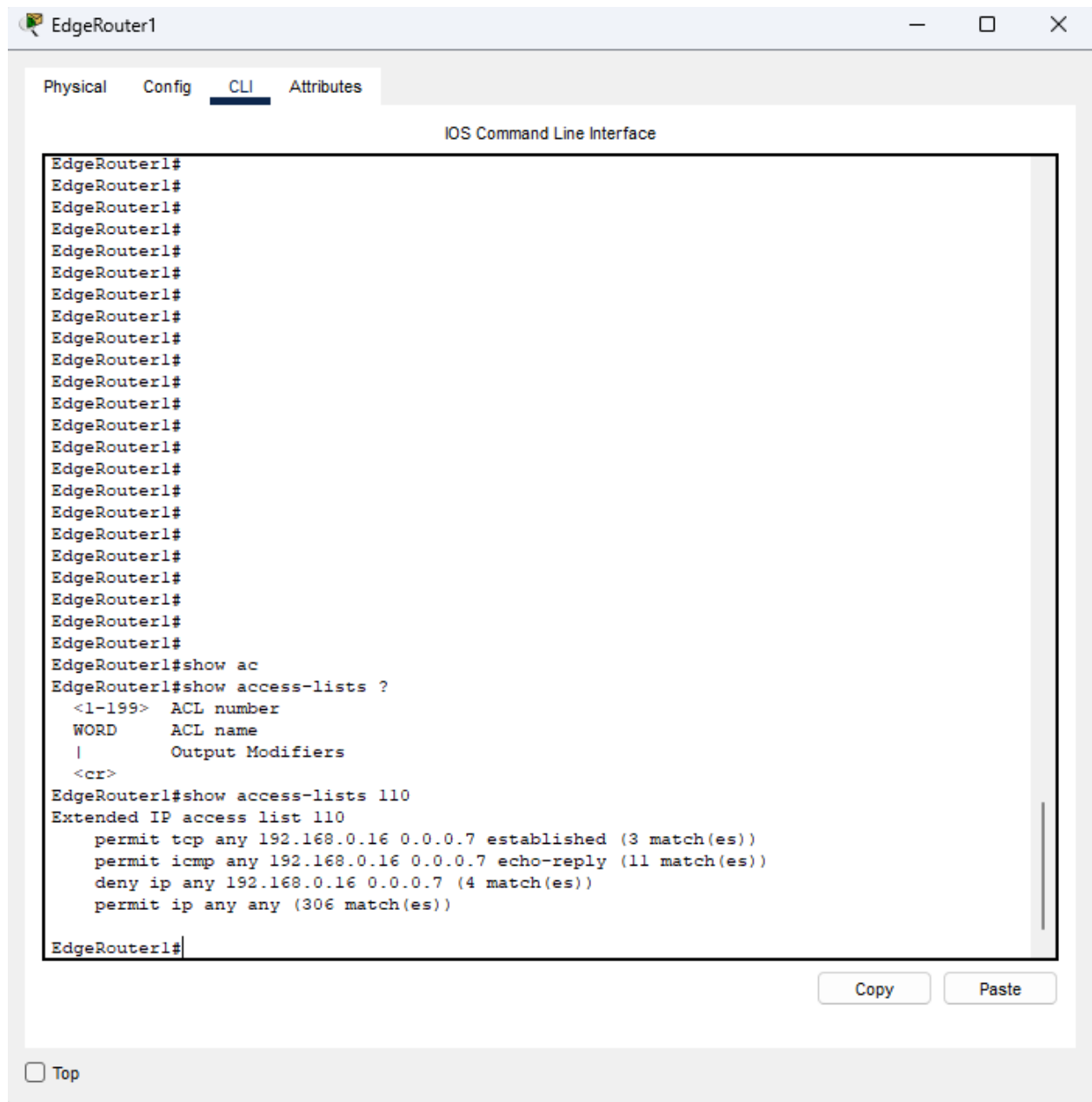


Deny ACL statement:

1. Access the web server's command prompt.
2. Ping the PC located on IT VLAN 10.
3. The destination should be unreachable.



4. Access the EdgeRouter1.
5. Display the access list (ACL 110 in this case).



6. The TCP, ICMP, and deny-any rules all show matches according to the tests performed. The match counts increase as you continue to ping or attempt additional connections.
7. This verifies that the packets were correctly evaluated by the ACL in each scenario.

Test Case #2: Administering an Access Control List for Guest Access

Your network must utilize an access control list that allows guest access. Guest access should be limited to internet traffic only.

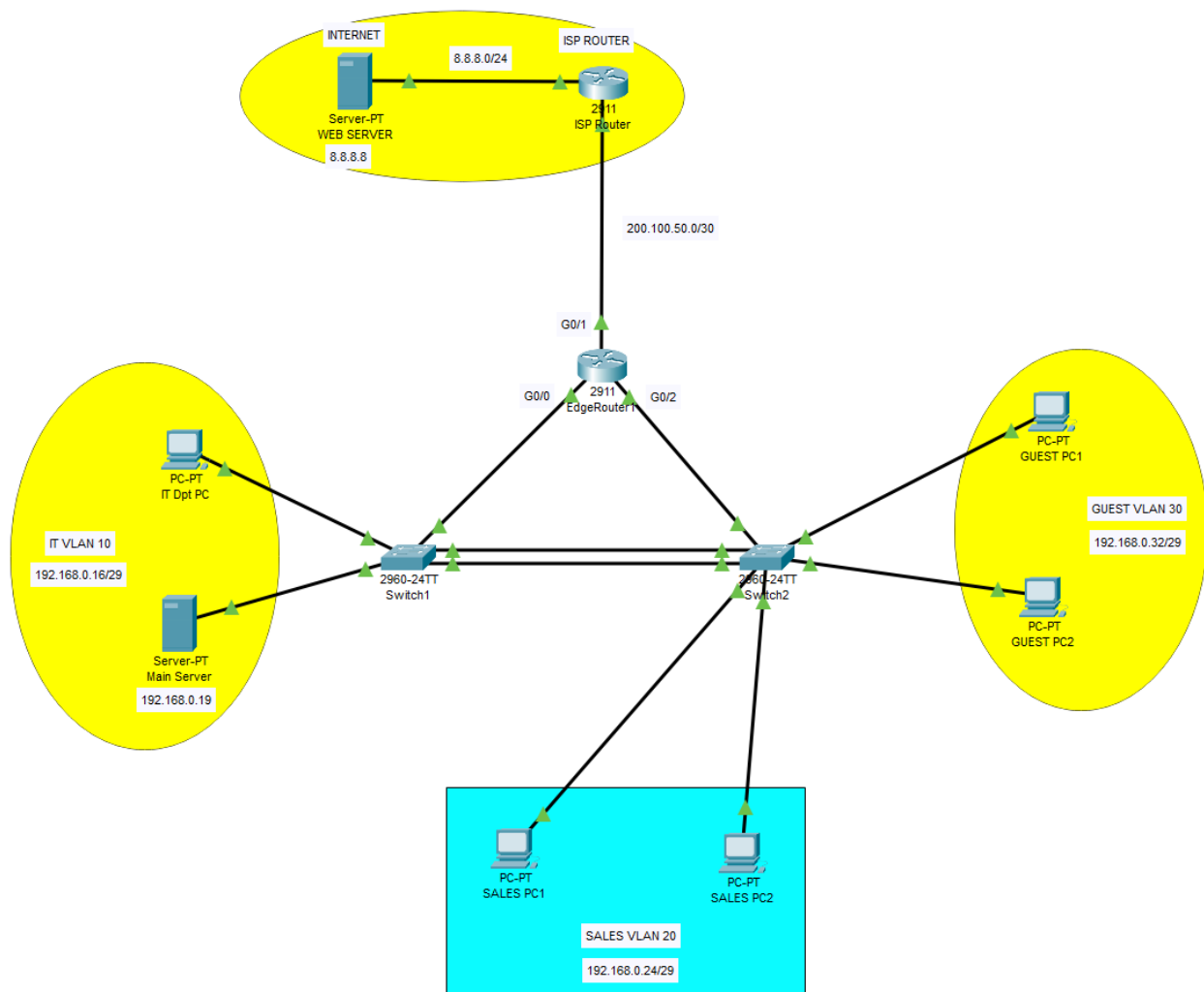
Functionality

Describe the **functionality** of the test case in relation to your network project. Identify the relevant tools (devices, subnets, etc.) used in this test case and their specific interactions.

The Guest VLAN has an access control list that restricts traffic to Internet access only for the IP address 8.8.8.8. It also includes a UDP rule that allows guest end devices to obtain DHCP leases from the main server at 192.168.0.19, located in the IT VLAN. All other traffic is denied.

Network Diagram or Segment

Provide a **network diagram or segment** visualizing the topology and devices used in this test case.



Testing Method

Summarize the **testing method** used to verify functionality of the network project within the virtual lab environment, including any metrics of success.

The following testing method will demonstrate that Guest PC1 can successfully ping the web server at IP address 8.8.8.8, while attempts to ping the main server at 192.168.0.19 will be unreachable. It is important to note that the UDP rule only allows Guest PC1 to obtain a DHCP lease from the server at 192.168.0.19, and all other traffic to that server is denied.

That is the reason the ping fails while DHCP requests still succeed.

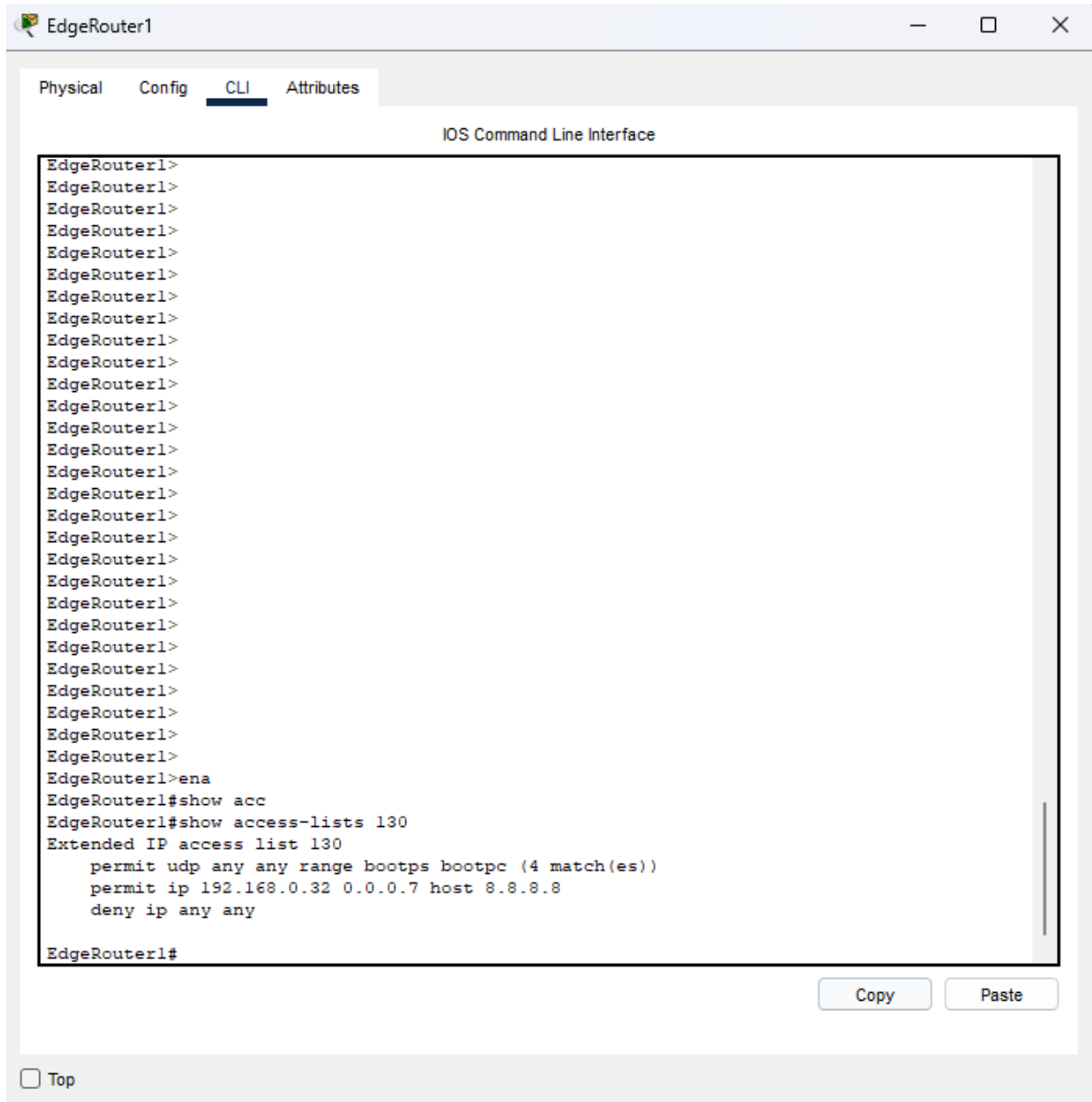
ACL 130 is assigned to the Guest VLAN and includes a permit rule allowing any device from the Guest VLAN subnet to access the host 8.8.8.8, a rule that allow UDP traffic for the DHCP server, and finally a deny-any rule to prevent Guest VLAN end devices from accessing other parts of the network.

Process List

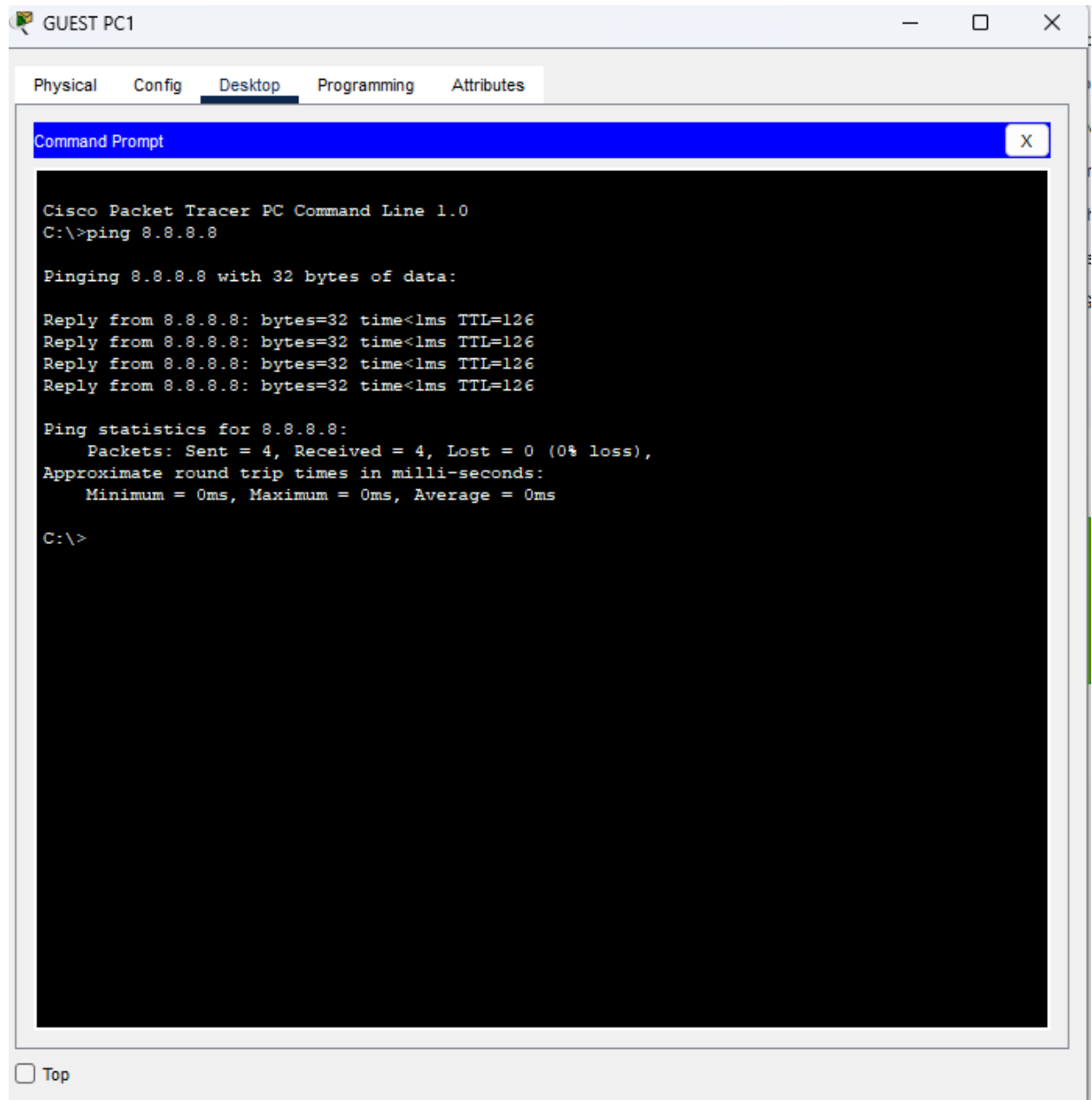
Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.

1. First, let's access the EdgeRouter1 to verify the existence of the access list assigned to Guest VLAN 30. In this case, it is ACL 130.
2. We will then check the match count to confirm that it increases after testing.



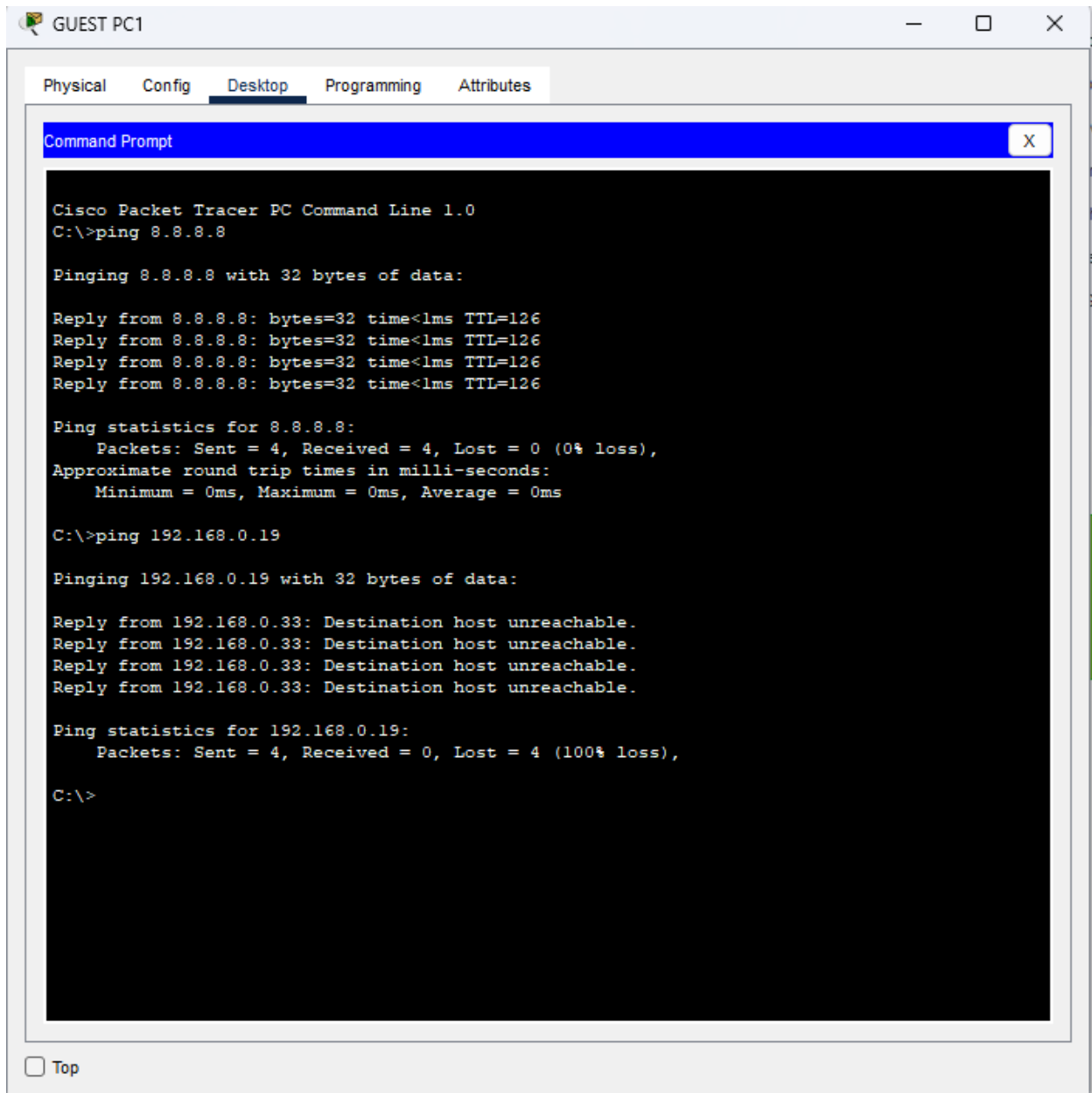


3. Access the Guest PC1 and open the command prompt.
4. Ping the web server at 8.8.8.8.
5. The destination should be reachable.



6. Now try to ping the main server at 192.168.0.19 from Guest PC1.
7. The ping should fail.





8. Now access EdgeRouter1 and display access list 130.
9. Verify that the match count has increased.



```
EdgeRouter1>
EdgeRouter1>
EdgeRouter1>
EdgeRouter1>
EdgeRouter1>
EdgeRouter1>
EdgeRouter1>
EdgeRouter1>
EdgeRouter1>
EdgeRouter1>
EdgeRouter1>
EdgeRouter1>
EdgeRouter1>
EdgeRouter1>
EdgeRouter1>
EdgeRouter1>
EdgeRouter1>
EdgeRouter1>
EdgeRouter1>
EdgeRouter1>
EdgeRouter1>
EdgeRouter1>ena
EdgeRouter1#show acc
EdgeRouter1#show access-lists 130
Extended IP access list 130
  permit udp any any range bootps bootpc (4 match(es))
  permit ip 192.168.0.32 0.0.0.7 host 8.8.8.8
  deny ip any any

EdgeRouter1#show access-lists 130
Extended IP access list 130
  permit udp any any range bootps bootpc (4 match(es))
  permit ip 192.168.0.32 0.0.0.7 host 8.8.8.8 (4 match(es))
  deny ip any any (4 match(es))

EdgeRouter1#
```

10. As shown in the picture above the permit rule for the host 8.8.8.8 increased 4 matches, reflecting the access to the web server. And the deny-any rule also increased 4 matches, reflecting the access to the main server at 192.168.0.19.



Test Case #3: Security Compliance—Log-in Banners

Display a log-in banner when accessing each device on the network. The log-in banner should notify users of an acceptable use policy (AUP) or other security-based policies when attempting to log into the network.

Functionality

*Describe the **functionality** of the test case in relation to your network project. Identify the relevant tools (devices, subnets, etc.) used in this test case and their specific interactions.*

To meet security compliance requirements, log-in banners were configured on EdgeRouter1 and on both Layer 2 switches. These banners display a message informing users of the acceptable use policy, warning that only authorized access is permitted, and that all activity is monitored. This ensures users are clearly notified of the organization's security policies before logging into any network infrastructure devices. The consistent application of these banners across all administrative interfaces supports organizational policy and helps prevent unauthorized use by providing an explicit notice upon connection.

Network Diagram or Segment

*Provide a **network diagram or segment** visualizing the topology and devices used in this test case.*

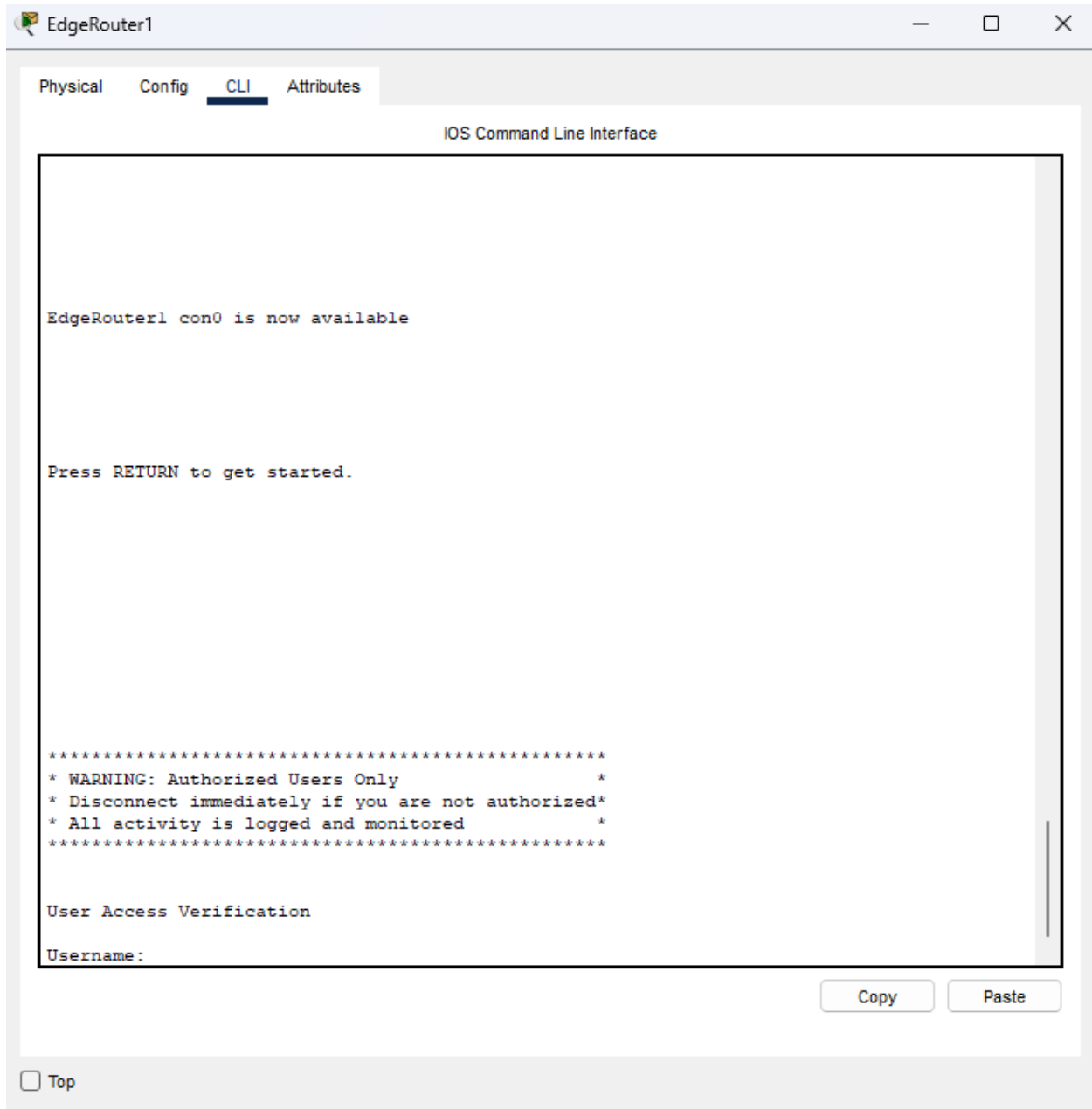




To verify the login banner functionality, the console connection was used to access EdgeRouter1, Switch1, and Switch2. Upon opening the console, the configured banner was displayed, confirming that the security notice was properly in place.

Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.

1. Log-in banners can be configured using the "banner motd" command.
2. These banners will appear whenever any user accesses the device, whether through the console or via SSH.
3. Access each device using the console connection.
4. A login-banner should be displayed before the authentication prompt.



Switch1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
*****
* Authorized Access Only - Monitored *
*****

User Access Verification

Username:
% Username: timeout expired!


Press RETURN to get started!


*****
* Authorized Access Only - Monitored *
*****

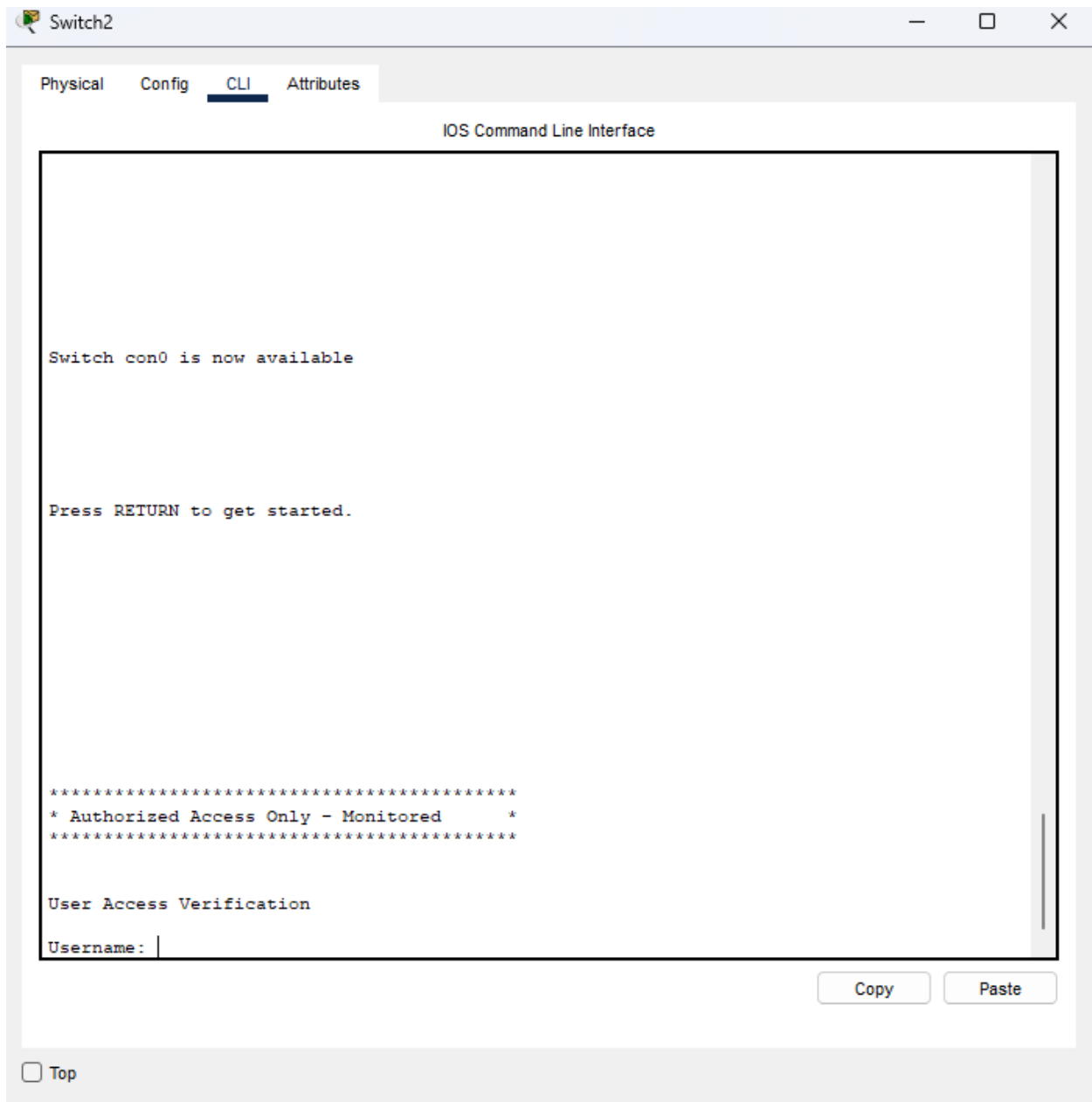
User Access Verification

Username: |
```

Copy Paste

☐ Top





Test Case #4: Accessing External Resources—Routing and Traffic Security

User devices on your network should have dynamic addresses that are assigned through DHCP unless they provide a service that requires a static address. You must also have at least one network resource that requires a static address.

Functionality

*Describe the **functionality** of the test case in relation to your network project. Identify the relevant tools (devices, subnets, etc.) used in this test case and their specific interactions.*

DHCP is properly assigned to the devices that best fit this configuration. Guest VLAN and Sales VLAN end devices should receive DHCP addresses from the main server. Static IP addresses are assigned to devices on the IT VLAN, such as the IT PC and the main server, for better management. Static IP addresses were also assigned to the web server and the ISP router that connects to the edge router.

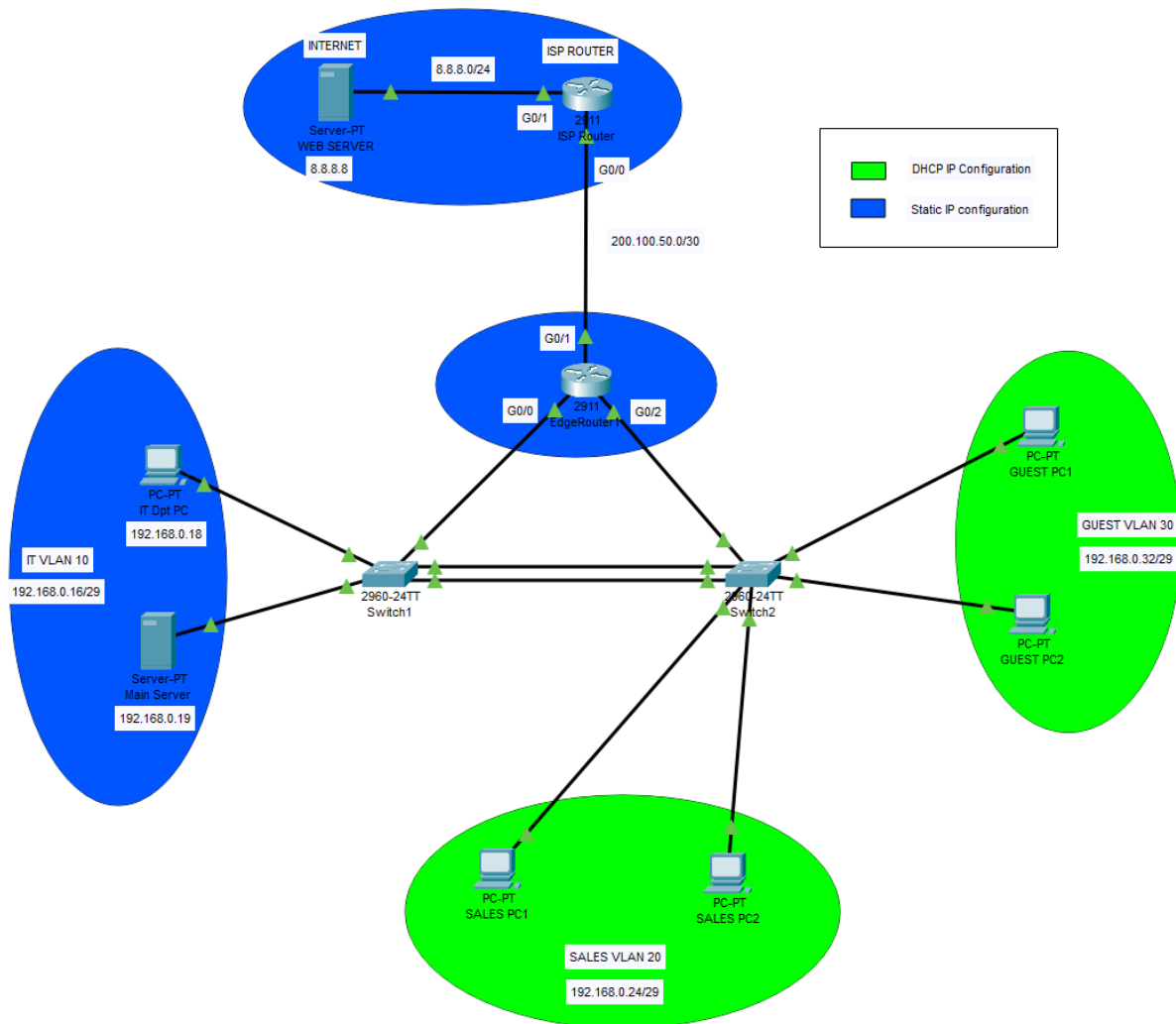
Static IP addresses configured:

IT PC – 192.168.0.18
Main Server – 192.168.0.19
EdgeRouter1 G0/1 – 200.100.50.1
ISP Router G0/0 – 200.100.50.2
ISP Router G0/1 – 8.8.8.1
Web Server – 8.8.8.8

Network Diagram or Segment

*Provide a **network diagram or segment** visualizing the topology and devices used in this test case.*





Testing Method

Summarize the **testing method** used to verify functionality of the network project within the virtual lab environment, including any metrics of success.

The DHCP service was configured on the main server, with separate DHCP pools assigned according to the subnet of each VLAN. The Guest VLAN and Sales VLAN end devices were tested by releasing and renewing their IP addresses to confirm they received the correct DHCP lease from the server. The test was considered successful if each device received an address within its designated subnet range, along with the correct default gateway, confirming proper DHCP functionality across those VLANs.

Process List

Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.



1. Access the main server to verify the DHCP server is on and pools are assigned for the Sales and Guest VLANs.

The screenshot shows the 'Main Server' configuration window with the 'Services' tab selected. The 'DHCP' service is enabled. The configuration fields are as follows:

- Interface: FastEthernet0
- Service: ☒ On
- Pool Name: GuestPool
- Default Gateway: 192.168.0.33
- DNS Server: 0.0.0.0
- Start IP Address: 192, 168, 0, 34
- Subnet Mask: 255, 255, 255, 248
- Maximum Number of Users: 5
- TFTP Server: 0.0.0.0
- WLC Address: 0.0.0.0

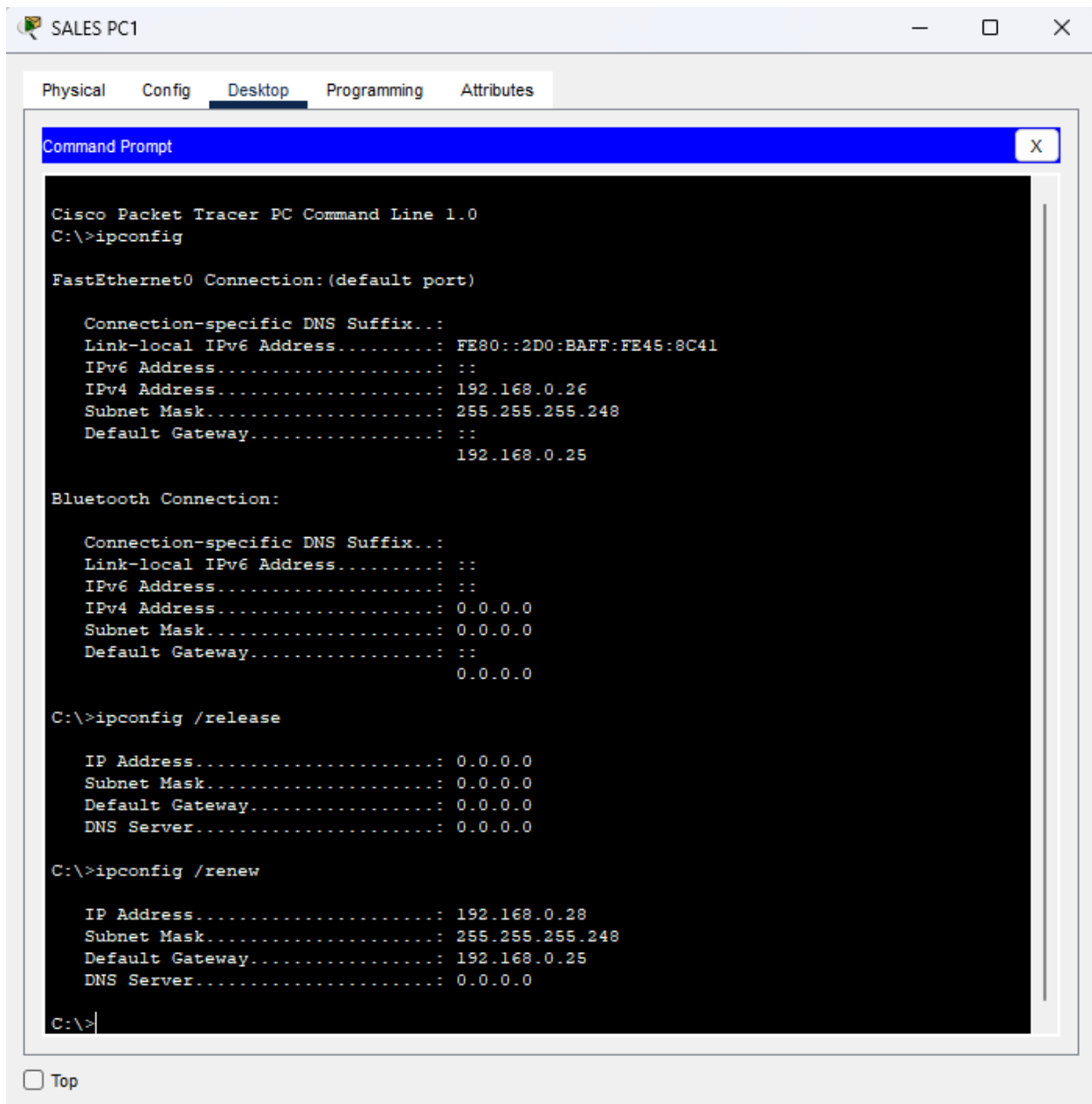
Below the configuration fields are buttons for 'Add', 'Save', and 'Remove'. A table lists the configured DHCP pools:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
GuestPool	192.168.0.33	0.0.0.0	192.168.0.34	255.255.255...	5	0.0.0.0	0.0.0.0
SalesPool	192.168.0.25	0.0.0.0	192.168.0.26	255.255.255...	5	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.0.16	255.255.255...	512	0.0.0.0	0.0.0.0

At the bottom left, there is a 'Top' button.

2. Access one PC from both Sales and Guest VLANs to test DHCP assignment.
3. Open the command prompt on each pc.
4. Type ipconfig to verify the current IP address.
5. Type ipconfig /release to remove the current IP address.
6. Type ipconfig /renew to obtain a new DHCP IP and confirm that DHCP is working.





SALES PC1

Physical Config **Desktop** Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2D0:BAFF:FE45:8C41
    IPv6 Address . . . . .: ::
    IPv4 Address. . . . .: 192.168.0.26
    Subnet Mask . . . . .: 255.255.255.248
    Default Gateway . . . . .: ::
                                192.168.0.25

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address. . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                0.0.0.0

C:\>ipconfig /release

IP Address. . . . .: 0.0.0.0
Subnet Mask . . . . .: 0.0.0.0
Default Gateway . . . . .: 0.0.0.0
DNS Server . . . . .: 0.0.0.0

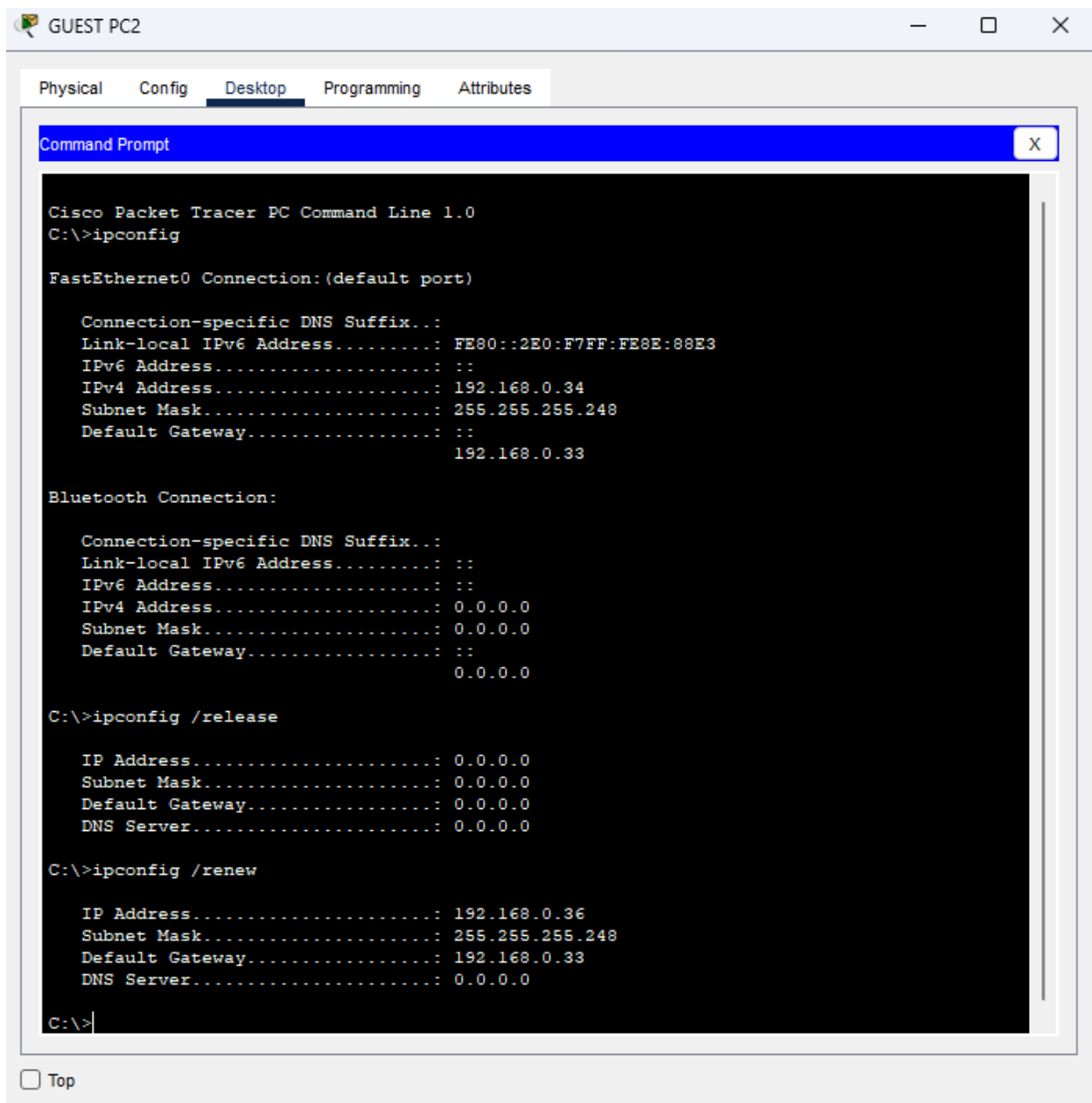
C:\>ipconfig /renew

IP Address. . . . .: 192.168.0.28
Subnet Mask . . . . .: 255.255.255.248
Default Gateway . . . . .: 192.168.0.25
DNS Server . . . . .: 0.0.0.0

C:\>
```

☐ Top





GUEST PC2

Physical Config **Desktop** Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2E0:F7FF:FE8E:88E3
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.0.34
    Subnet Mask . . . . .: 255.255.255.248
    Default Gateway . . . . .: ::
                                192.168.0.33

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                0.0.0.0

C:\>ipconfig /release

    IP Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: 0.0.0.0
    DNS Server . . . . .: 0.0.0.0

C:\>ipconfig /renew

    IP Address . . . . .: 192.168.0.36
    Subnet Mask . . . . .: 255.255.255.248
    Default Gateway . . . . .: 192.168.0.33
    DNS Server . . . . .: 0.0.0.0

C:\>
```

☐ Top



Test Case #5: Layer 2 Link Redundancy and Spanning Tree Protocol (802.1w)

Enable and manage the Spanning Tree Protocol to establish redundant Layer 2 paths while avoiding possible loops and broadcast storms. Identify the Layer 2 devices that will become the root bridge.

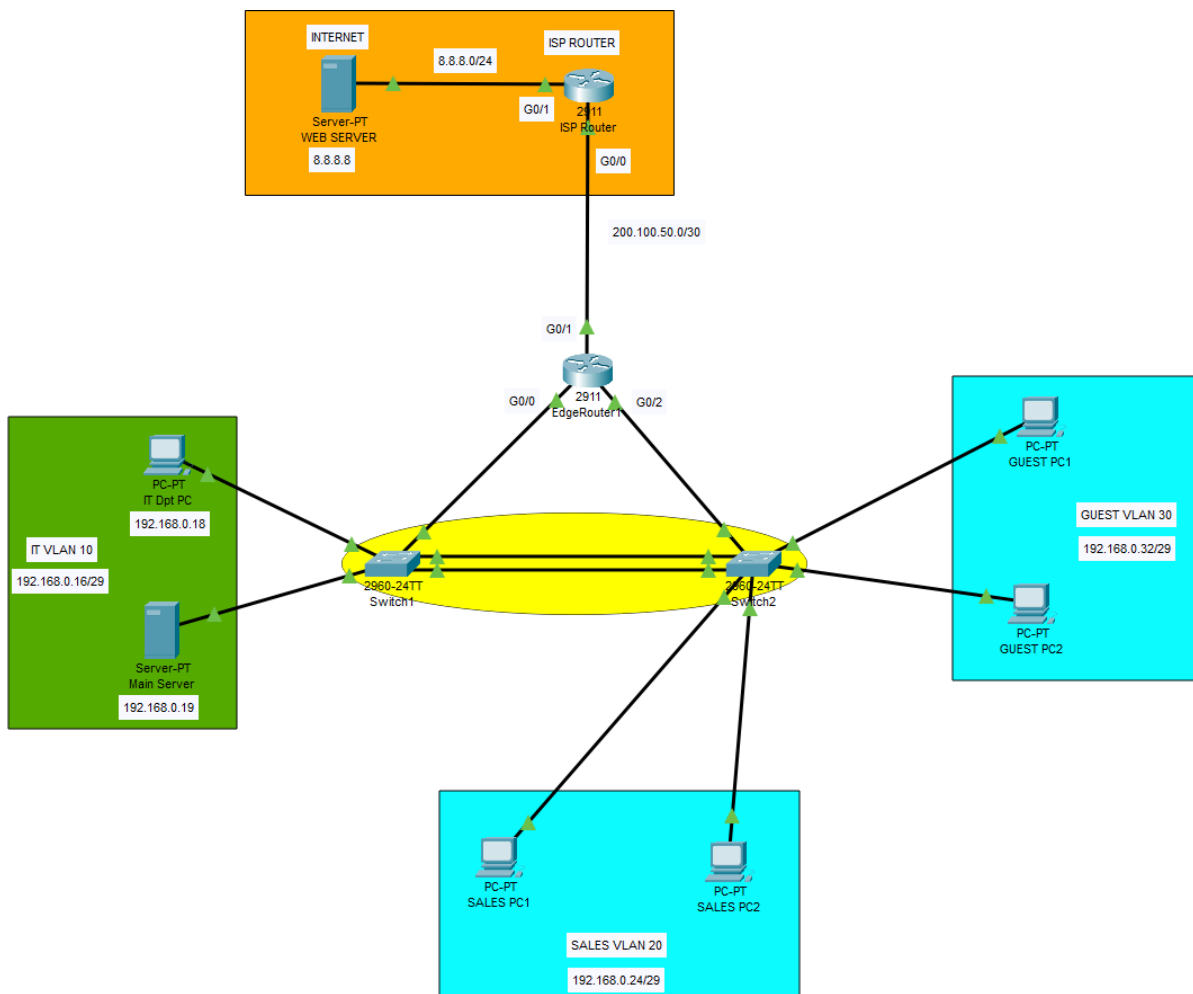
Functionality

Describe the **functionality** of the test case in relation to your network project. Identify the relevant tools (devices, subnets, etc.) used in this test case and their specific interactions.

Spanning Tree Protocol (802.1w) was enabled on both Layer 2 switches to prevent loops and maintain redundancy in the Layer 2 network. One switch was selected as the root bridge to ensure predictable forwarding paths and rapid recovery in case of a link failure.

Network Diagram or Segment

Provide a **network diagram or segment** visualizing the topology and devices used in this test case.



Testing Method

Summarize the **testing method** used to verify functionality of the network project within the virtual lab environment, including any metrics of success.

The spanning tree configuration was verified using the show spanning-tree command on both switches to confirm the root bridge, port roles, and blocking states. The EtherChannel between Switch1 and Switch2 was maintained, and a third separate trunk link was added to introduce redundant paths. As a functional test, the EtherChannel was administratively shut down to observe STP reconvergence, which successfully transitioned the third link to become the new root port, maintaining network connectivity without broadcast storms or switching loops after the topology change.

Process List

Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.

1. Access Switch1 and Switch2 and use the "show spanning-tree" command to verify that STP is enabled and identify the root bridge switch.



Switch1
_ □ ×

Physical Config CLI Attributes

IOS Command Line Interface

```

1003 c1net-default active
Switch#
Switch#
Switch#
Switch#show sp
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
            Address     0004.9AB2.B6DB
            Cost        12
            Port        27 (Port-channel1)
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
            Address     000C.CF11.8A25
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  20

Interface    Role Sts Cost      Prio.Nbr Type
-----
Fa0/3        Desg FWD 19        128.3    P2p
Fa0/4        Desg FWD 19        128.4    P2p
Fa0/5        Desg FWD 19        128.5    P2p
Fa0/8        Altn BLK 19        128.8    P2p
Pol          Root FWD 12        128.27   Shr

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
            Address     0004.9AB2.B6DB
            Cost        136
            Port        27 (Port-channel1)
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

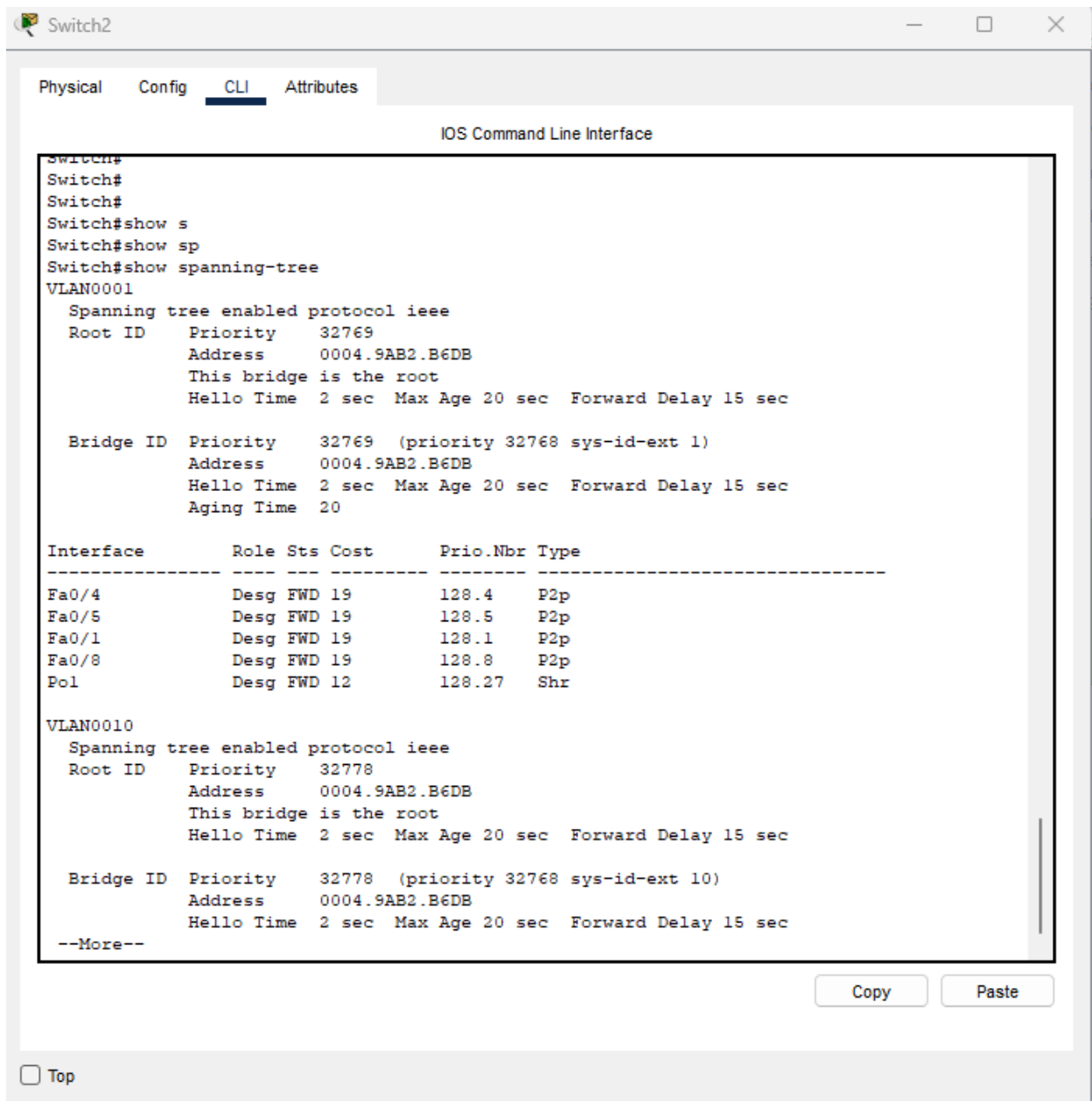
  Bridge ID  Priority    32778 (priority 32768 sys-id-ext 10)
  --More--

```

Copy Paste

☐ Top





2. The root bridge, as we can see in the "Root ID" section, is Switch2.
3. For this functionality test, we added the Fa0/8 link between both switches so it acts as a second redundant link. We can verify that Po1 (The EtherChannel link) is the root port on Switch1 and is in the forwarding state, while Fa0/8 is in the blocking state.
4. Administratively shut down port Po1 to simulate a link failure.
5. Access Switch1 and verify the spanning tree protocol again.



Switch1

Physical Config **CLI** Attributes

IOS Command Line Interface

```

VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority    32798

Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
                Address    0004.9AB2.B6DB
                Cost        19
                Port        8(FastEthernet0/8)
                Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
                Address    000C.CF11.8A25
                Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
                Aging Time  20

Interface                Role Sts Cost      Prio.Nbr Type
-----
Fa0/3                    Desg FWD 19        128.3    P2p
Fa0/4                    Desg FWD 19        128.4    P2p
Fa0/5                    Desg FWD 19        128.5    P2p
Fa0/8                    Root FWD 19        128.8    P2p
Pol                       Desg FWD 12        128.27   Shr

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
                Address    0004.9AB2.B6DB
                Cost        19
                Port        8(FastEthernet0/8)
                Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778 (priority 32768 sys-id-ext 10)
--More--

```

Copy Paste

☐ Top

- Verify that Fa0/8 transitioned to the root port and went into the forwarding state to maintain connectivity.



Test Case #6: Edge Device Syslog and NTP

Configure perimeter devices to generate system logs that capture unwanted traffic. Additionally, those perimeter devices should utilize Network Time Protocol (NTP) for clock synchronization.

***NOTE:** Packet Tracer's limited logging capabilities can sometimes pose a challenge when trying to simulate a real-world scenario for capturing unwanted traffic and generating system logs. Below are some alternative solutions to satisfying the test case.

1. Use an External Syslog Server:

- **Set up a simple syslog server:** You can use a Linux machine or a virtual machine to do this.
- **Configure your Packet Tracer devices:** Tell your devices to send their logs to this external server.
- **Analyze logs:** This gives you more flexibility to analyze logs and troubleshoot issues.
- **Document your work.**

2. Focus on ACLs and Verification:

Even though Packet Tracer might not log ACL violations directly, you can still:

- **Configure ACLs:** Set up rules to block unwanted traffic.
- **Verify the ACLs:** Use Packet Tracer's packet capture or simulation tools to check if the ACLs are working as expected.
- **Document your work:** Explain your ACL configuration and the verification process.

Items to be included in the documentation:

- Clearly document the limitations of Packet Tracer's logging capabilities.
- Explain the alternative method used to assess unwanted traffic detection.
- Emphasize your understanding of the desired logging behavior and how you would implement it in a real-world scenario.

Functionality

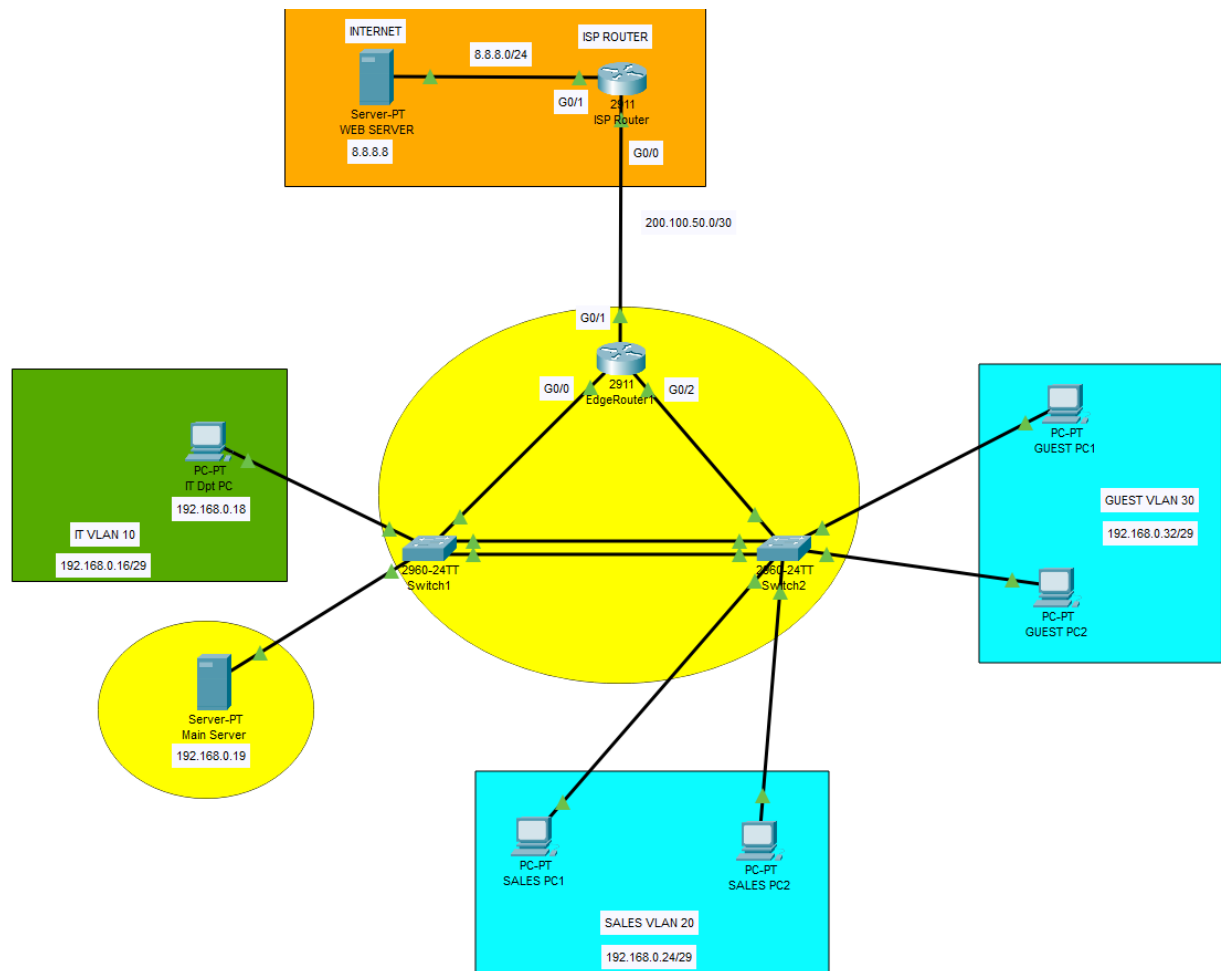
*Describe the **functionality** of the test case in relation to your network project. Identify the relevant tools (devices, subnets, etc.) used in this test case and their specific interactions.*

The perimeter devices were configured to send system logs to the Main Server acting as a Syslog server, allowing monitoring of events such as interface status changes and routing updates. Additionally, NTP was configured as well to synchronize its clock with the Main Server, ensuring accurate timestamping of logs.



Network Diagram or Segment

Provide a **network diagram or segment** visualizing the topology and devices used in this test case.



Testing Method

Summarize the **testing method** used to verify functionality of the network project within the virtual lab environment, including any metrics of success.

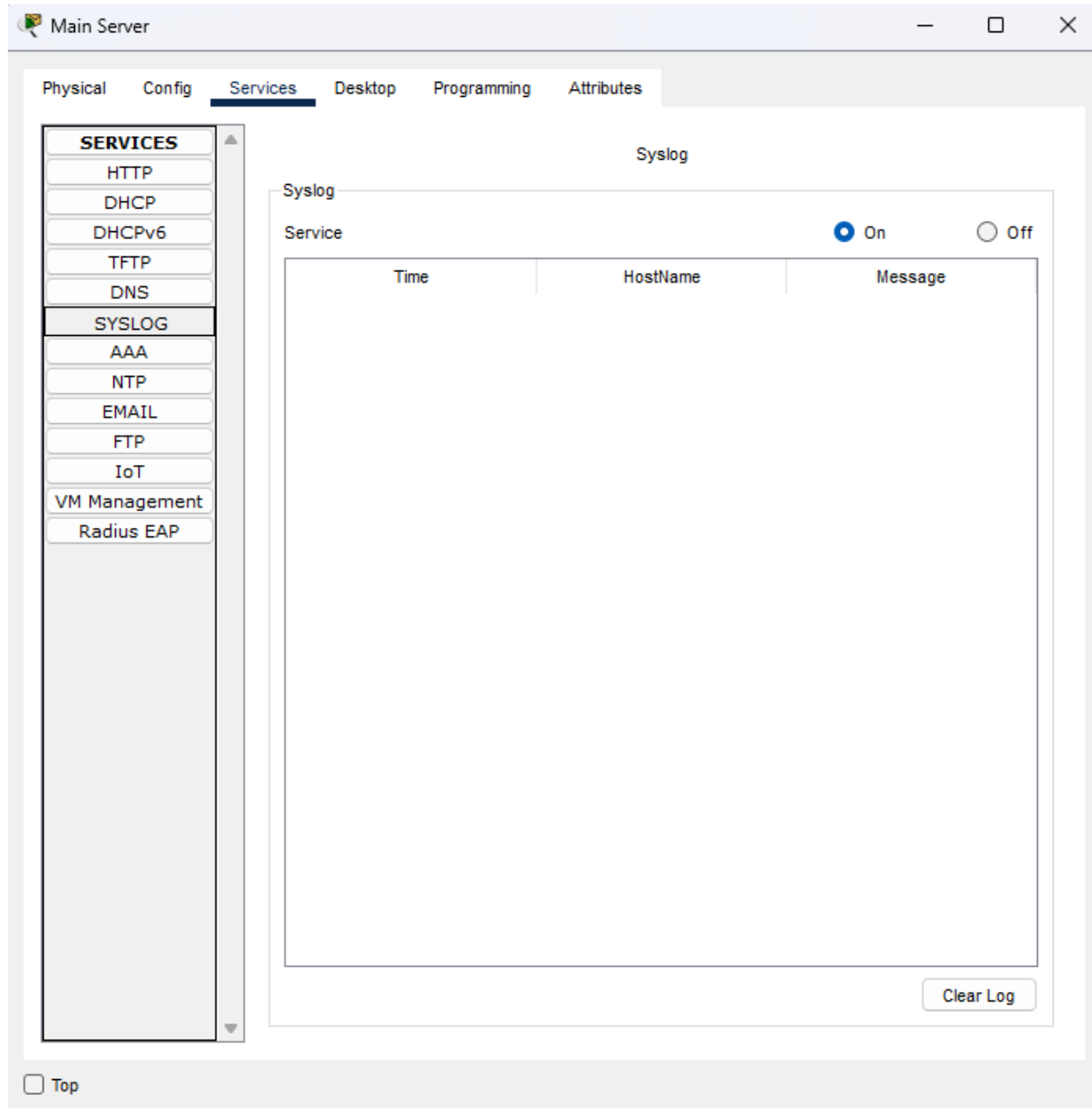
The syslog and NTP testing will be performed on the EdgeRouter. The interface shutdown and re-enable commands will be executed on the EdgeRouter to generate syslog messages, which will then be verified on the Main Server. NTP functionality will also be checked from the EdgeRouter using the `show ntp associations` command to confirm synchronization.



Process List

Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.

1. Open the main server and verify that Syslog and NTP services are on.
2. Make sure the time in the NTP service is set to the actual time.



The screenshot shows the 'Main Server' configuration window with the 'Services' tab selected. The left sidebar lists various services, with 'NTP' highlighted. The main area shows the NTP service configuration, including a 'Service' status set to 'On', an 'Authentication' section with 'Disable' selected, and a calendar for June 2025. The calendar shows the current date as 05:26:28PM.

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP**
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

NTP

Service: ☒ On ☐ Off

Authentication:

☐ Enable ☒ Disable

Key: Password:

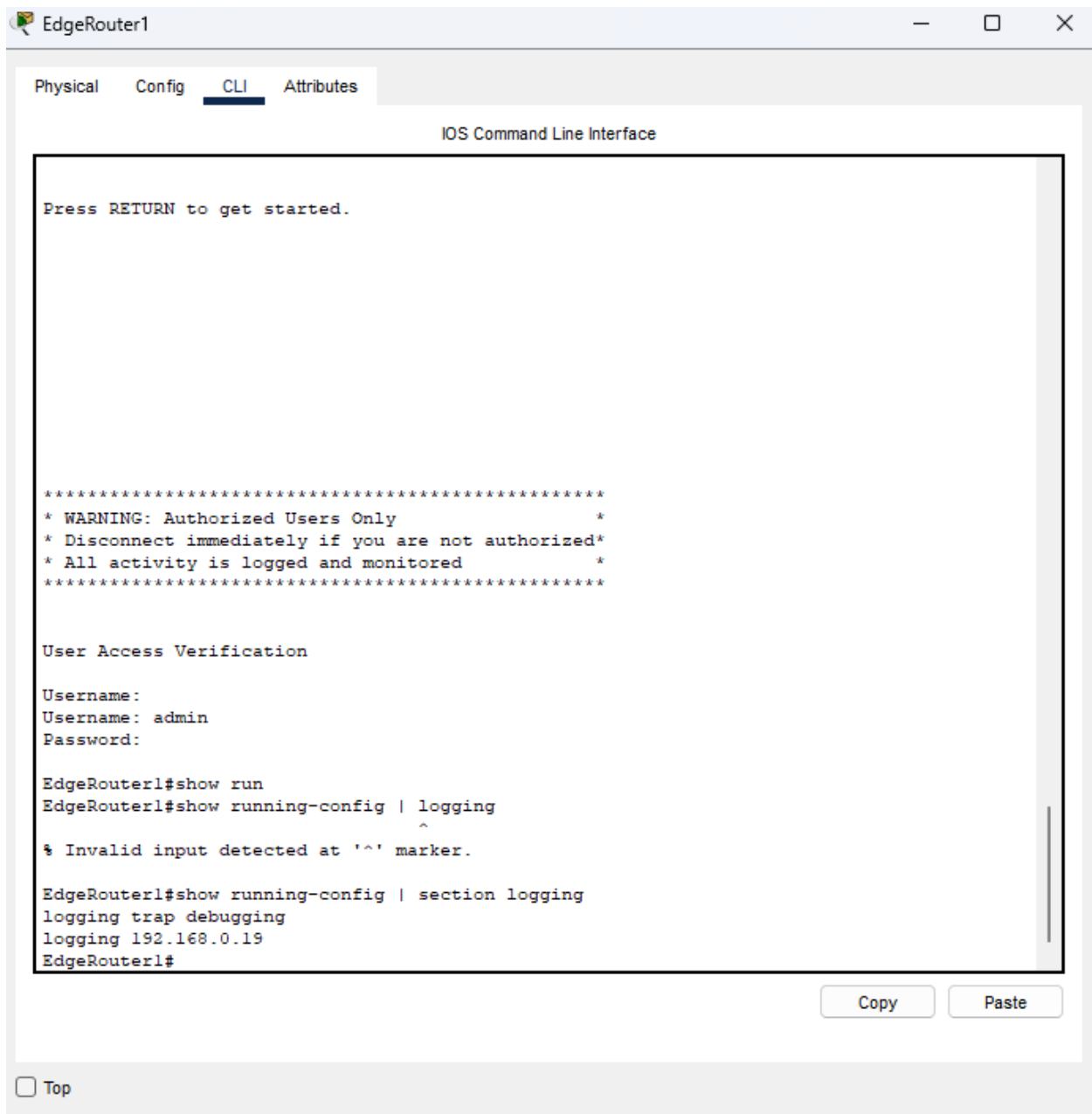
June 2025 05:26:28PM

Sun	Mon	Tue	Wed	Thu	Fri	Sat
25	26	27	28	29	30	31
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5

☐ Top

3. "Logging <syslog-server-ip>" command is used to configure the perimeter devices with the syslog server.
4. "ntp server <ntp-server-ip>" command is used to configure the perimeter devices with the NTP server to synchronize the device's clock.
5. Access the EdgeRouter1 and verify logging is configured.





6. For the functional test, shut down and up port G0/1 and check the syslog server to verify logging.



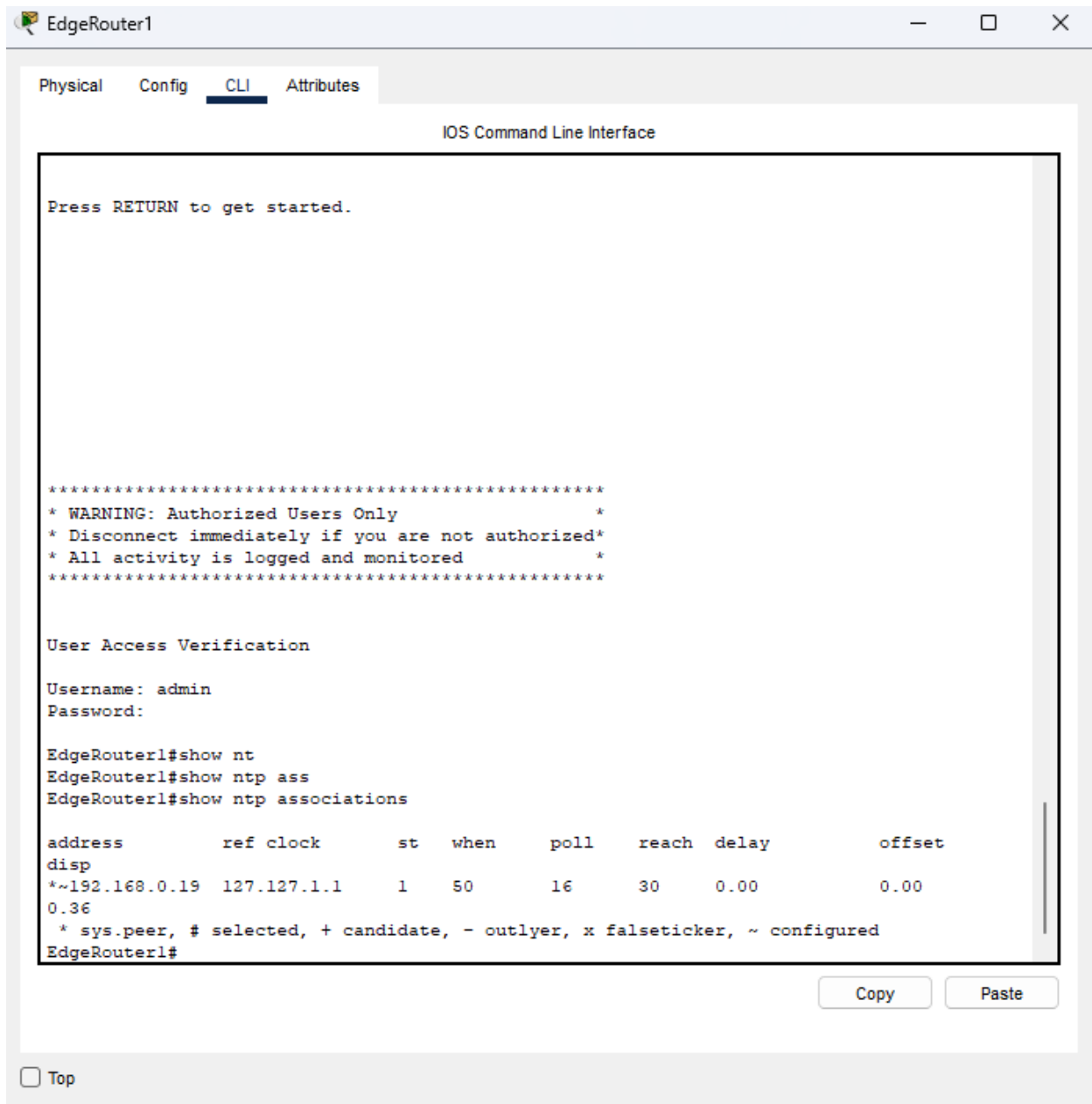
The screenshot shows the 'Main Server' configuration window with the 'Services' tab selected. The 'Syslog' service is configured and enabled. The Syslog table displays the following entries:

Service	Time	HostName	Message
1	-	192.168.0.17	%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
2	-	192.168.0.17	%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
3	-	192.168.0.17	17:34:45: %OSPF-5-ADJCHG: Process 30, Nbr 2.2.2.2 on GigabitEthernet0/1 from FULL to ...
4	-	192.168.0.17	%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
5	-	192.168.0.17	%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
6	-	192.168.0.17	%SYS-5-CONFIG_I: Configured from console by console

The interface also includes a 'Clear Log' button at the bottom right of the Syslog table.

7. Access the EdgeRouter1 and verify that NTP is configured using "show ntp associations".





8. NTP is configured with the IP 192.168.0.19 that is the IP of the main server.
9. Use "show clock" to verify the date and time matches with the NTP server.



EdgeRouter1

Physical Config **CLI** Attributes

IOS Command Line Interface

Press RETURN to get started.

* WARNING: Authorized Users Only *
* Disconnect immediately if you are not authorized*
* All activity is logged and monitored *

User Access Verification

Username: admin
Password:

EdgeRouter1#show nt
EdgeRouter1#show ntp ass
EdgeRouter1#show ntp associations

address	ref clock	st	when	poll	reach	delay	offset
disp *~192.168.0.19	127.127.1.1	1	50	16	30	0.00	0.00
0.36							

* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

EdgeRouter1#show clock
*17:40:47.350 UTC Mon Jun 30 2025
EdgeRouter1#

Copy Paste

☐ Top



Main Server

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP**
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

NTP

Service ☒ On ☐ Off

Authentication

☐ Enable ☒ Disable

Key: Password:

June 2025 05:41:05PM

Sun	Mon	Tue	Wed	Thu	Fri	Sat
25	26	27	28	29	30	31
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5

☐ Top



Test Case #7: Basic Network Segmentation at Layer 2 via VLANs and 802.1q

Your network traffic should be segmented per department or service function at Layer 2 to enhance security and reduce network congestion at the switching layer while allowing segmented traffic to traverse between switches (VLAN trunking).

Functionality

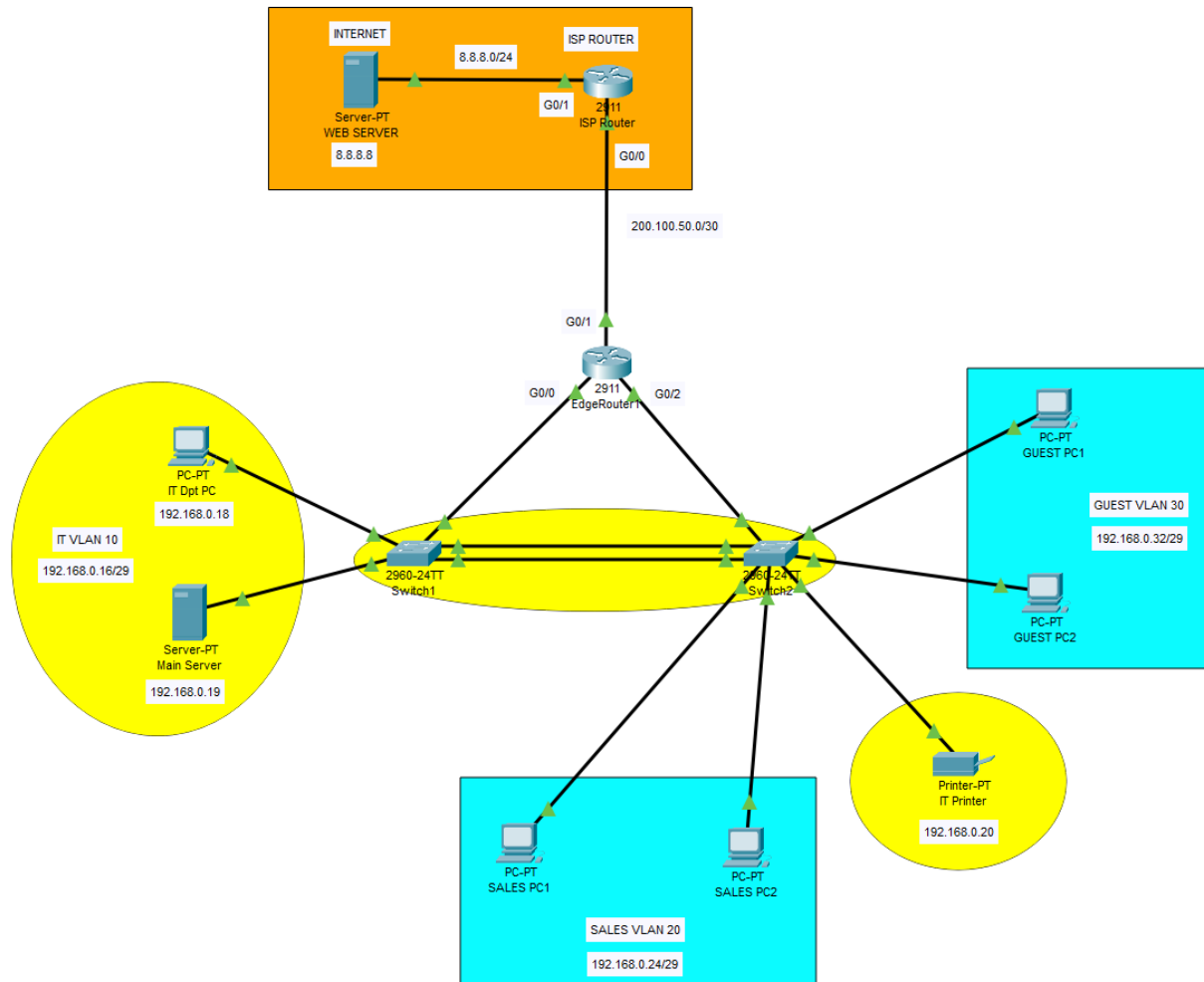
*Describe the **functionality** of the test case in relation to your network project. Identify the relevant tools (devices, subnets, etc.) used in this test case and their specific interactions.*

The network was segmented into multiple VLANs to separate traffic by department or function, reducing congestion and improving security at Layer 2. VLAN trunking (802.1Q) was configured between the switches to allow VLAN traffic to traverse properly. As long as matching VLANs are created on both switches, the trunk link ensures seamless communication between devices in the same VLAN across switches.

Network Diagram or Segment

*Provide a **network diagram or segment** visualizing the topology and devices used in this test case.*





Testing Method

Summarize the **testing method** used to verify functionality of the network project within the virtual lab environment, including any metrics of success.

As a functionality test, an IT printer was added to Switch2 with the same VLAN as the IT devices on Switch1. This verified that the trunk link between switches was successfully allowing VLAN traffic to pass, confirming proper Layer 2 segmentation and inter-switch VLAN connectivity.



Process List

Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.

1. Access Switch1 and Switch2.
2. Use "show vlan brief" command to confirm that the IT VLAN is configured on both switches.
3. Use "show interfaces trunk" to confirm trunk ports between Switch1 and Switch2 in this case across the Port-Channel 1.

Switch1

Physical Config **CLI** Attributes

IOS Command Line Interface

```

*****
* Authorized Access Only - Monitored *
*****

User Access Verification

Username:
Username: admin
Password:

Switch#show vl
Switch#show vlan bri
Switch#show vlan brief

```

VLAN	Name	Status	Ports
1	default	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2
10	IT	active	Fa0/1, Fa0/2
20	Sales	active	
30	Guest	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Switch#

Copy Paste

☐ Top



Switch2

Physical Config **CLI** Attributes

IOS Command Line Interface

```
*****
* Authorized Access Only - Monitored *
*****

User Access Verification

Username: admin
Password:

Switch#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
10	IT	active	Fa0/8
20	Sales	active	Fa0/2, Fa0/3
30	Guest	active	Fa0/6, Fa0/7
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Switch#

☐ Top



Switch1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Switch#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2
10	IT	active	Fa0/1, Fa0/2
20	Sales	active	
30	Guest	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
Switch#show int
Switch#show interfaces tr
Switch#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Pol	on	802.1q	trunking	1
Fa0/5	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Pol	10,20,30
Fa0/5	10,20,30

Port	Vlans allowed and active in management domain
Pol	10,20,30
Fa0/5	10,20,30

Port	Vlans in spanning tree forwarding state and not pruned
Pol	10,20,30
Fa0/5	10,20,30

Switch#

Copy Paste

☐ Top



Switch2

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Switch#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
10	IT	active	Fa0/8
20	Sales	active	Fa0/2, Fa0/3
30	Guest	active	Fa0/6, Fa0/7
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
Switch#show int
Switch#show interfaces tr
Switch#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Pol	on	802.1q	trunking	1
Fa0/1	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Pol	10,20,30
Fa0/1	10,20,30

Port	Vlans allowed and active in management domain
Pol	10,20,30
Fa0/1	10,20,30

Port	Vlans in spanning tree forwarding state and not pruned
Pol	10,20,30
Fa0/1	10,20,30

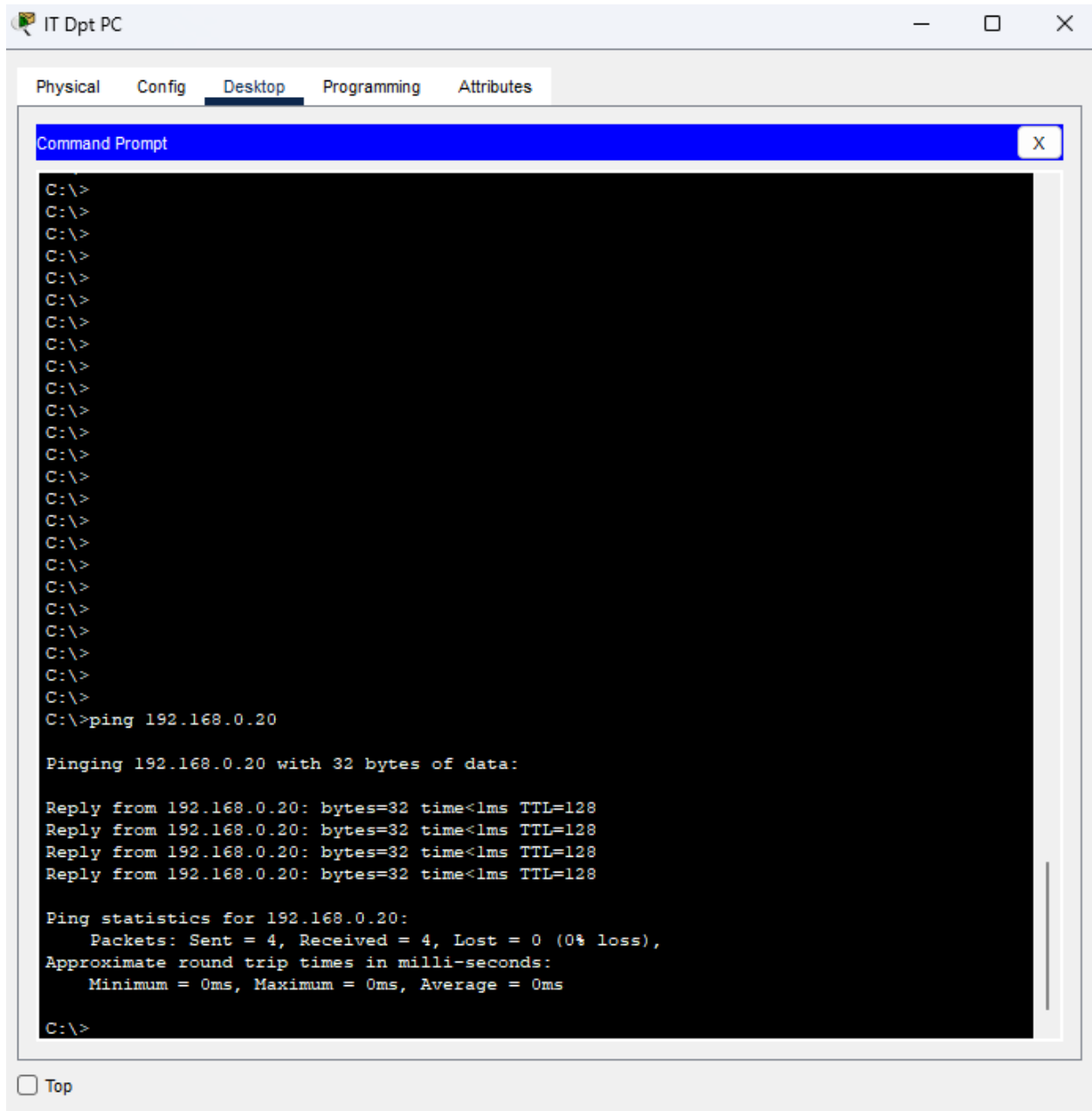
Switch#

Copy Paste

☐ Top

- The printer is connected to Fa0/8 port on Switch2.
- Ensure the port for the IT printer is configured in access mode and assigned to VLAN 10.
- Set an static IP on the printer for testing purposes, making sure it is within the same subnet as IT VLAN 10.
- Verify connectivity by testing from the IT PC to the printer.





Test Case #8: Basic or Advanced Networking

Custom Test Case

Your network will implement EtherChannel between core switches to provide redundancy and increase bandwidth. This configuration allows multiple physical links to act as a single logical connection. Improving performance and fault tolerance. If one link fails, traffic continues to flow through the remaining links without interruption.

Functionality

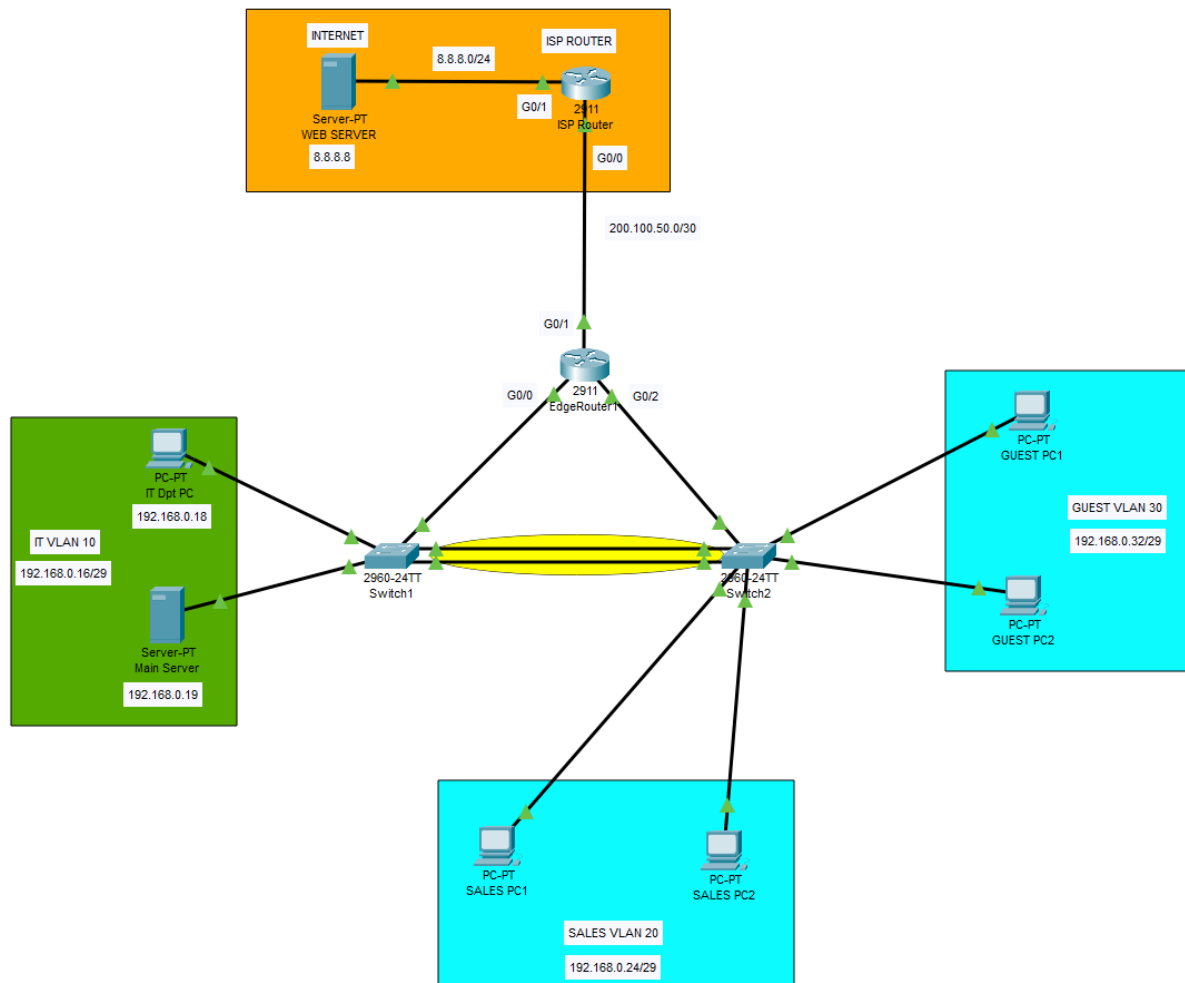
*Describe the **functionality** of the test case in relation to your network project. Identify the relevant tools (devices, subnets, etc.) used in this test case and their specific interactions.*

EtherChannel was implemented between the two core switches to aggregate multiple physical links into a single logical connection. This configuration improves bandwidth utilization and provides redundancy in case of a link failure. In this project, two FastEthernet links were grouped using LACP to form a port-channel between Switch1 and Switch2. This setup ensures continuous connectivity and prevents network disruptions if one of the physical links goes down.

Network Diagram or Segment

*Provide a **network diagram or segment** visualizing the topology and devices used in this test case.*





Testing Method

Summarize the **testing method** used to verify functionality of the network project within the virtual lab environment, including any metrics of success.

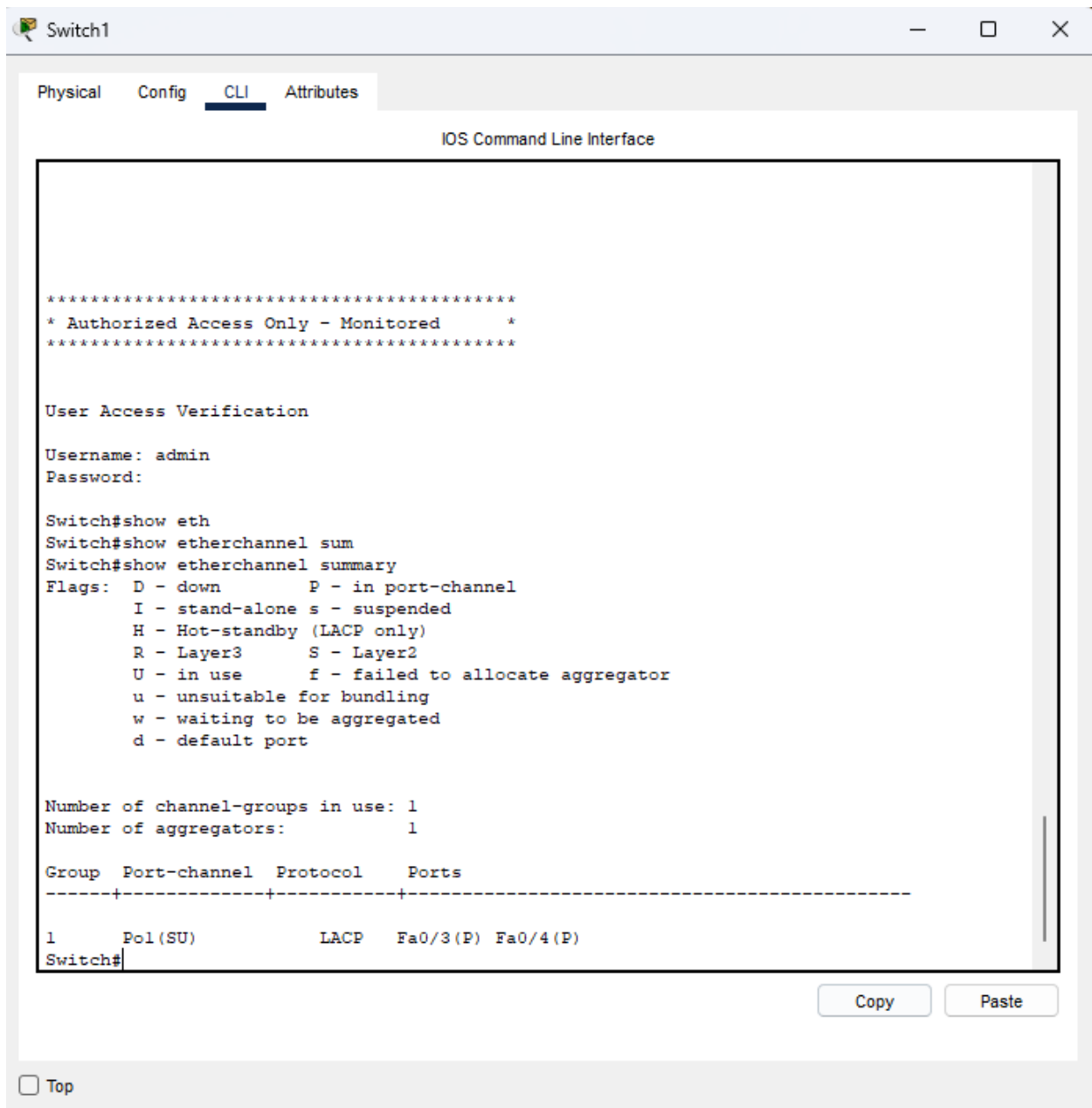
To verify EtherChannel functionality, I first confirmed the port-channel status using the "show etherchannel summary" command on both switches. Then, I tested connectivity between devices on each side of the EtherChannel to ensure traffic passed through successfully. As a fault-tolerance test, one of the physical member links was administratively shut down to simulate a failure. I verified that the port-channel remained operational through the remaining active link without dropping connectivity. The test was considered successful if no interruption occurred during the link failure simulation.



Process List

Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.

1. Access Switch1 and Switch2.
2. Verify EtherChannel Status using command "show etherchannel summary".



Switch2
— □ ×

Physical
Config
CLI
Attributes

IOS Command Line Interface

```

Press RETURN to get started!

*****
* Authorized Access Only - Monitored *
*****

User Access Verification

Username: admin
Password:

Switch#show eth
Switch#show etherchannel sum
Switch#show etherchannel summary
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Pol(SU)        LACP       Fa0/4(P) Fa0/5(P)
Switch#

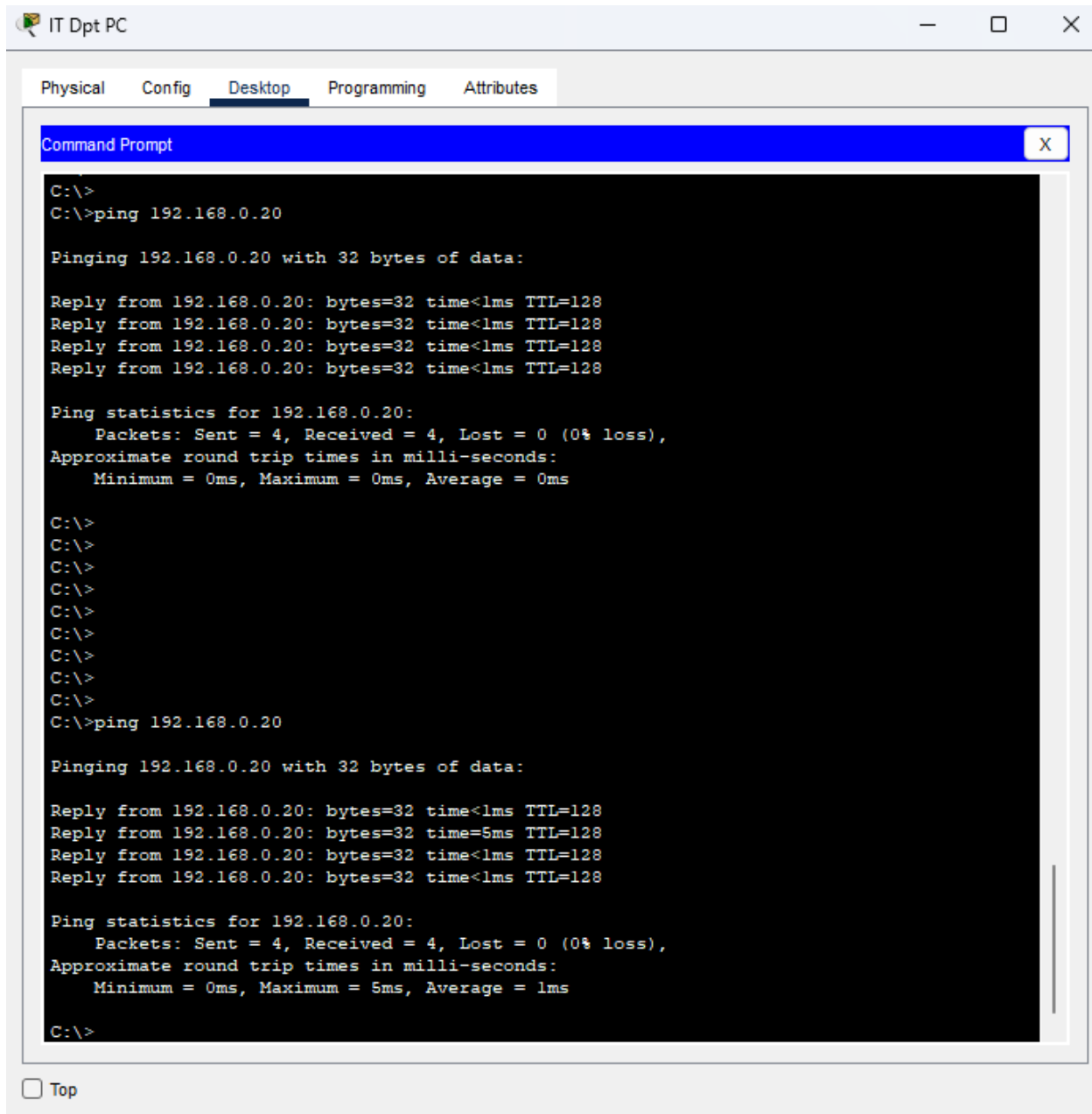
```

Copy
Paste

☐ Top

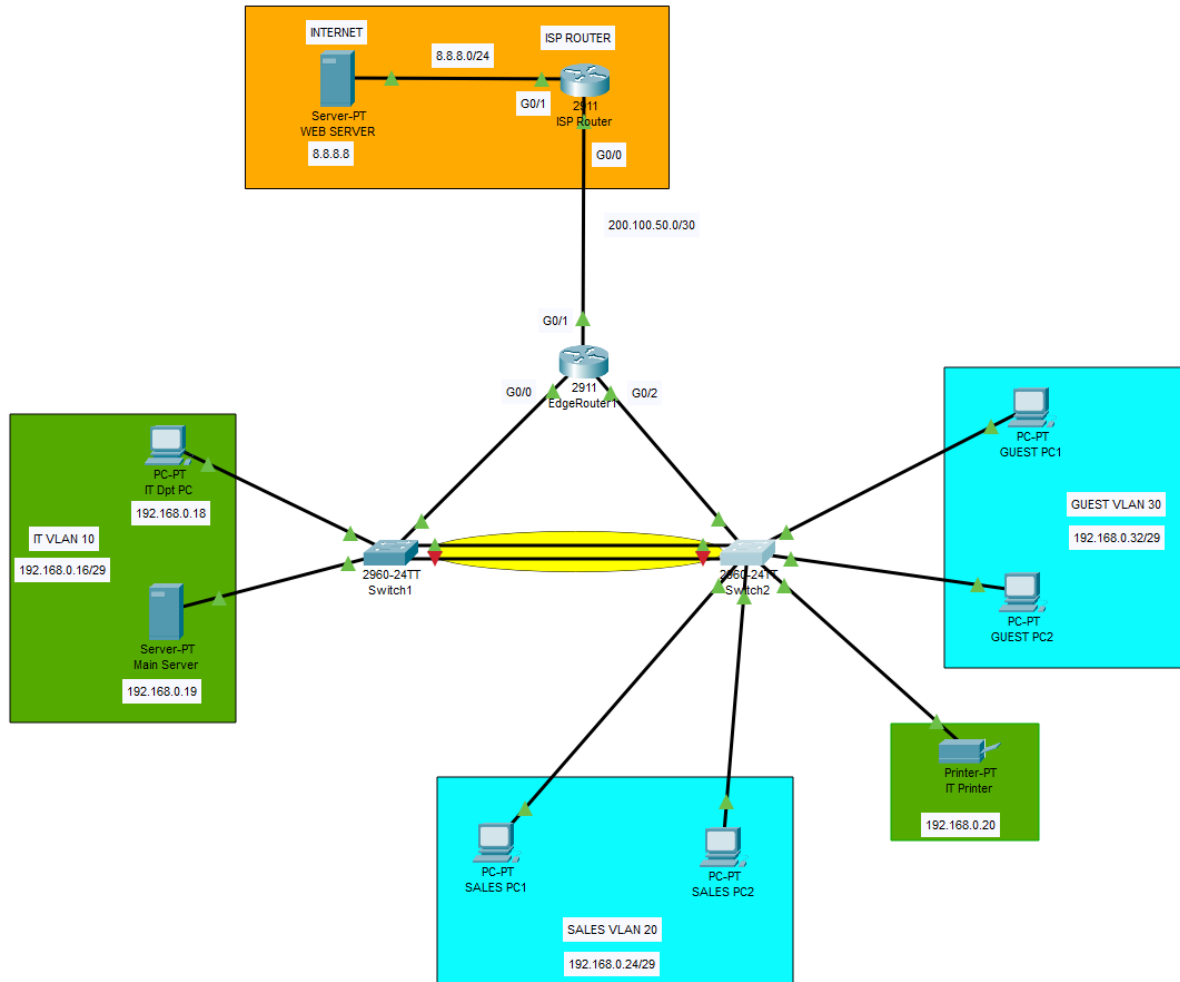
3. Ping across the EtherChannel from the IT VLAN. The printer can be added again for testing purposes, since the EtherChannel is configured as a trunk.





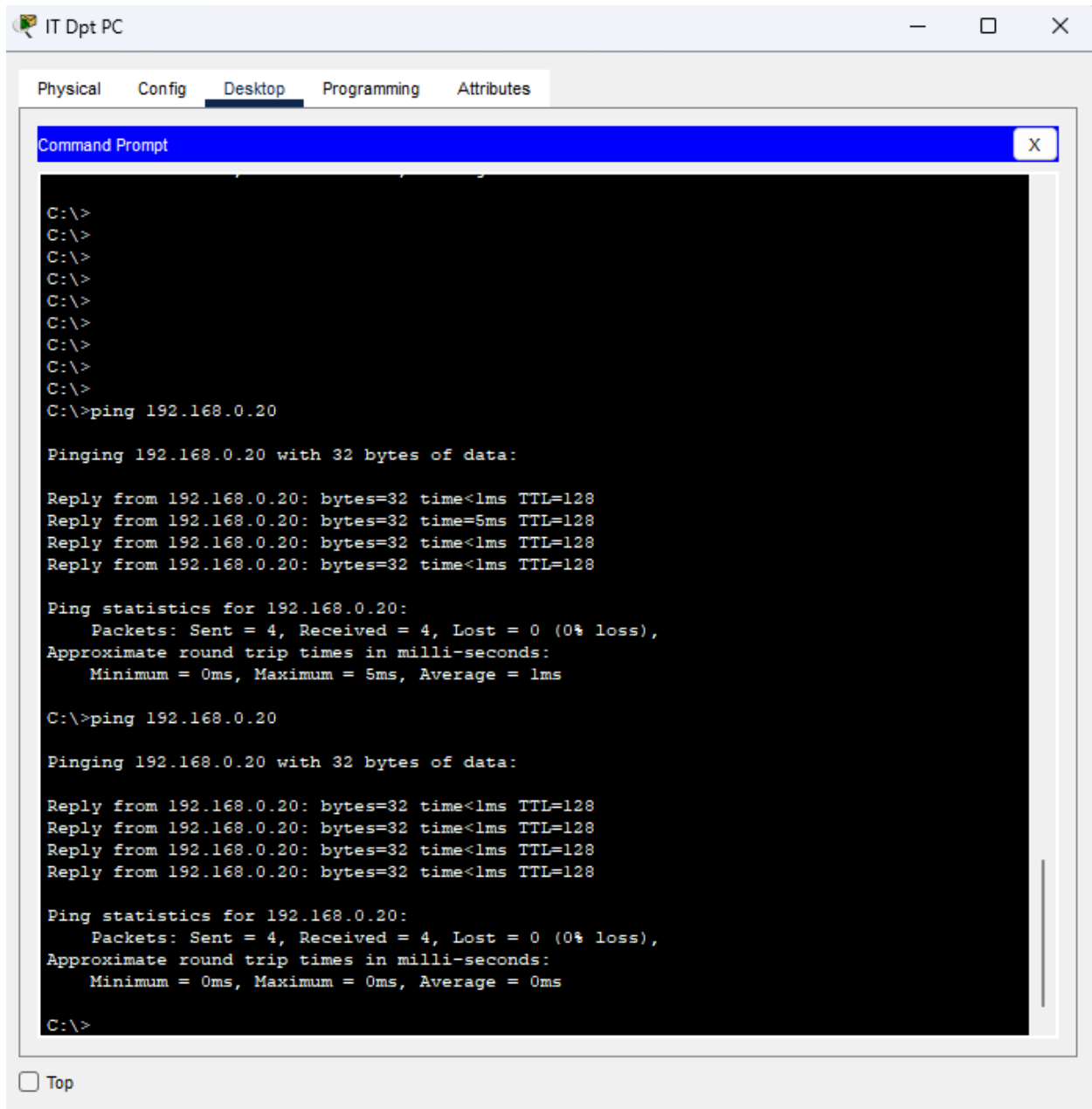
4. Administratively shut down a port on Switch2, in this case, I disabled port Fa0/5.





- Ping across the Etherchannel once again, the test should pass, proving link redundancy.





Test Case #9: Remote Access

Custom Test Case

Remote access will be secured using SSH (Secure Shell) configured on the router. SSH enables administrators to securely access and manage devices remotely. It will provide encrypted communication to prevent credential theft and unauthorized access.

Functionality

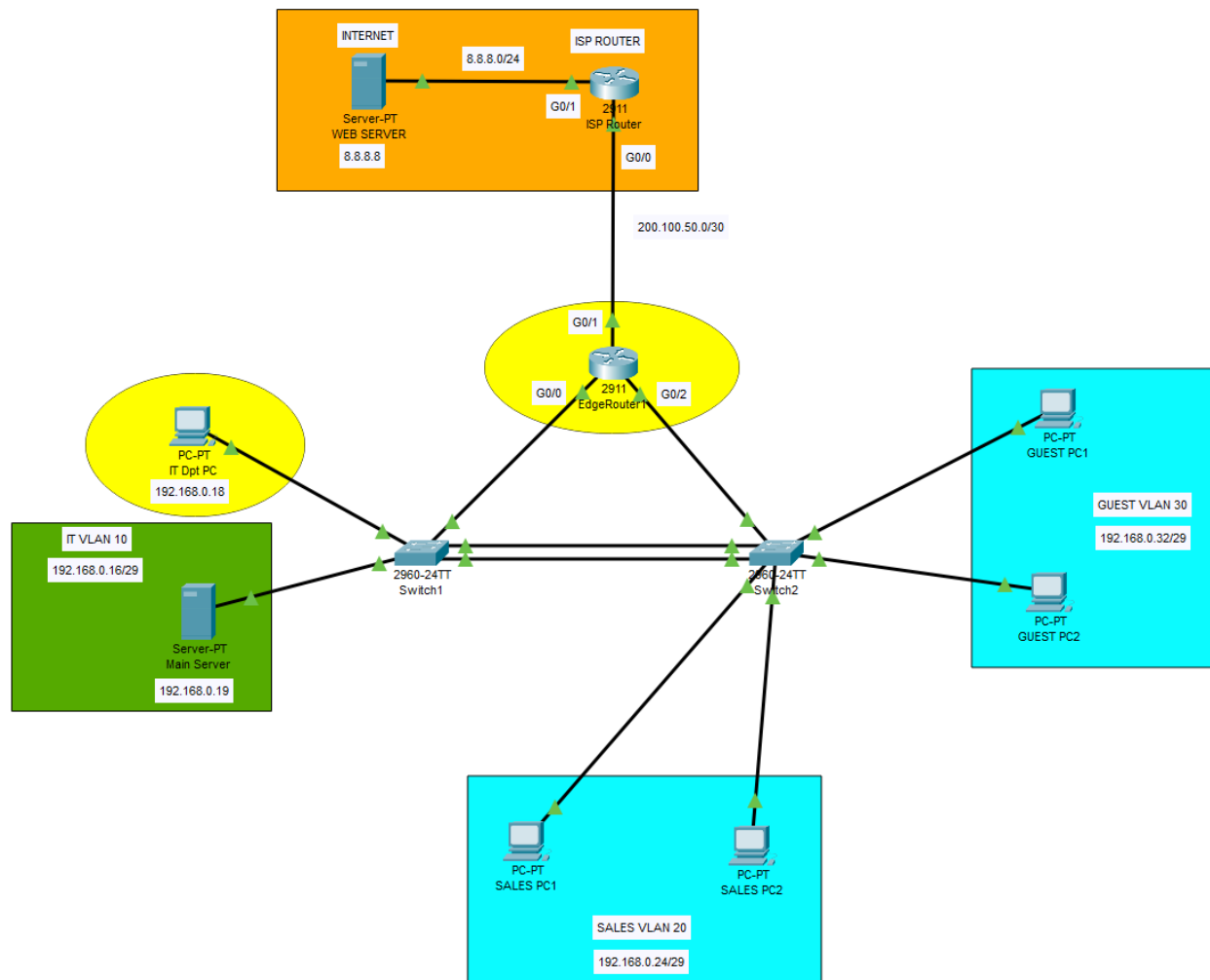
*Describe the **functionality** of the test case in relation to your network project. Identify the relevant tools (devices, subnets, etc.) used in this test case and their specific interactions.*

SSH was configured on the EdgeRouter1 to allow secure, encrypted remote access for administrative management. A domain name and local user credentials were set up. The router's vty lines were configured to accept SSH connections. This setup supports secure remote configuration, protecting credentials from interception and maintaining device integrity.

Network Diagram or Segment

*Provide a **network diagram or segment** visualizing the topology and devices used in this test case.*





Testing Method

Summarize the **testing method** used to verify functionality of the network project within the virtual lab environment, including any metrics of success.

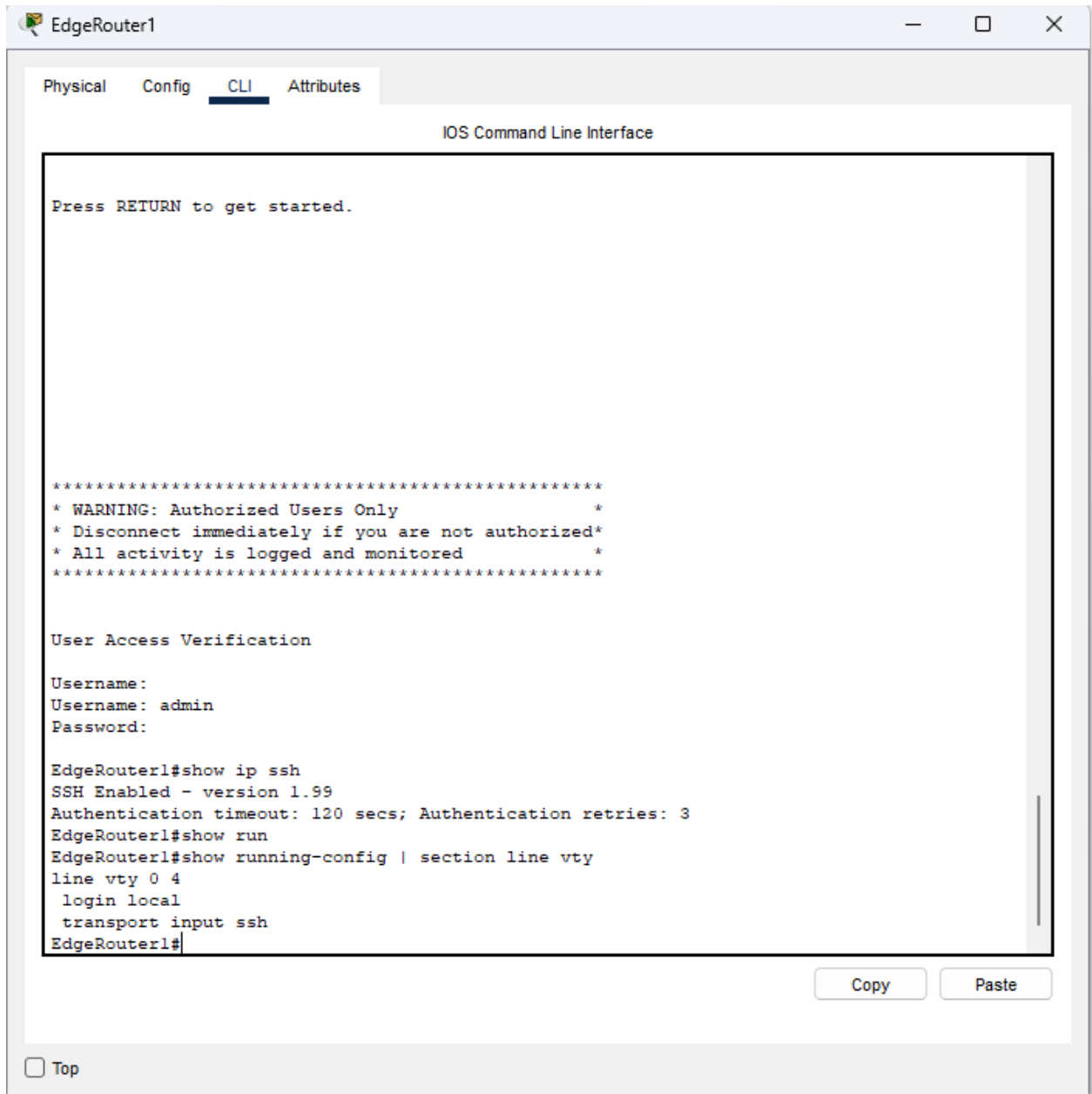
SSH functionality was tested by attempting to connect from a PC on the IT VLAN to the EdgeRouter1 using an SSH client. The connection was verified by successfully authenticating with the configured username and password, ensuring secure remote management was active and working as expected. The gateway of VLAN 10 for the SSH connection.



Process List

Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.

1. Verify that the EdgeRouter1 has SSH configured with a local username and password
2. Confirm that VTY lines are set to use SSH and have login local enabled.



The screenshot shows the CLI interface of EdgeRouter1. The 'CLI' tab is selected, and the 'IOS Command Line Interface' is displayed. The interface shows the following text:

```
Press RETURN to get started.
```

```
*****  
* WARNING: Authorized Users Only *  
* Disconnect immediately if you are not authorized*  
* All activity is logged and monitored *  
*****
```

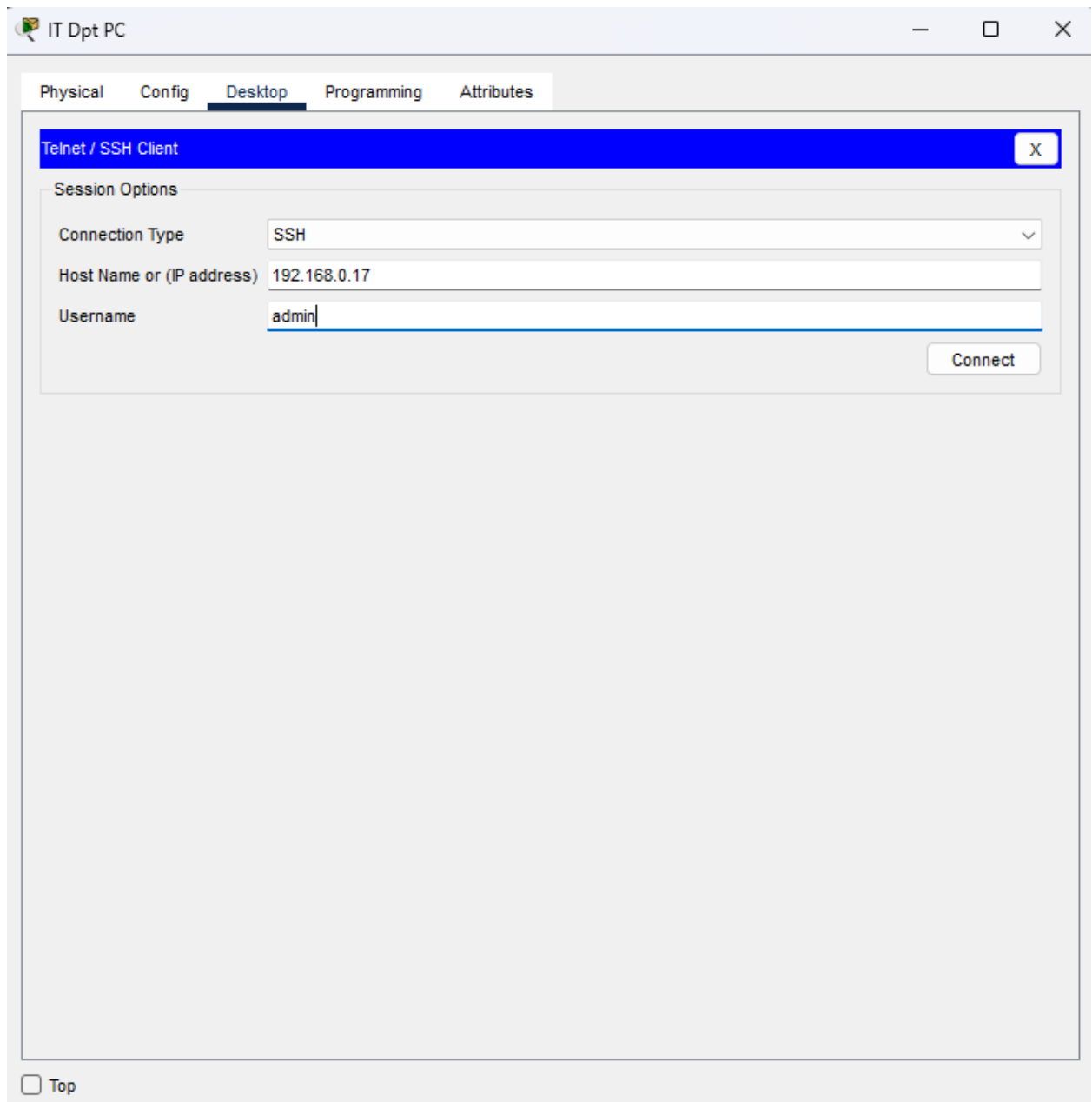
```
User Access Verification  
  
Username:  
Username: admin  
Password:
```

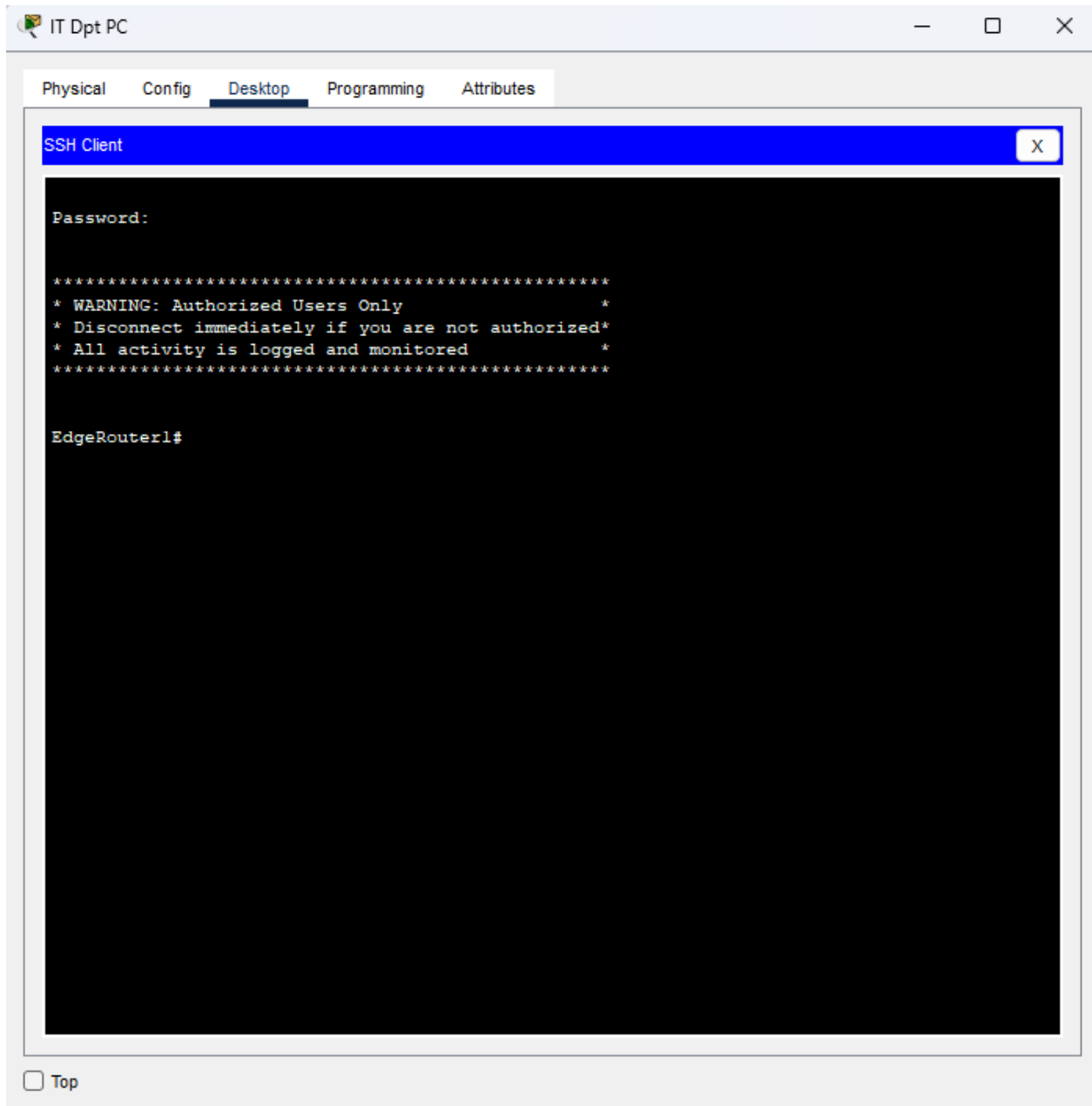
```
EdgeRouter1#show ip ssh  
SSH Enabled - version 1.99  
Authentication timeout: 120 secs; Authentication retries: 3  
EdgeRouter1#show run  
EdgeRouter1#show running-config | section line vty  
line vty 0 4  
  login local  
  transport input ssh  
EdgeRouter1#
```

At the bottom of the window, there are 'Copy' and 'Paste' buttons, and a 'Top' link.



3. From a PC in the IT VLAN, open the command prompt.
4. Use the "ssh" command to connect to the EdgeRouter1 IP address.
5. Enter the correct username and password when prompted.
6. Confirm connection.





Test Case #10: Network Security

Custom Test Case

Implement port security on the Layer 2 switch that connects Guest VLAN devices. This will restrict unauthorized access by limiting the number of MAC addresses allowed. This prevents unauthorized devices from accessing the network by only allowing known endpoints.

Functionality

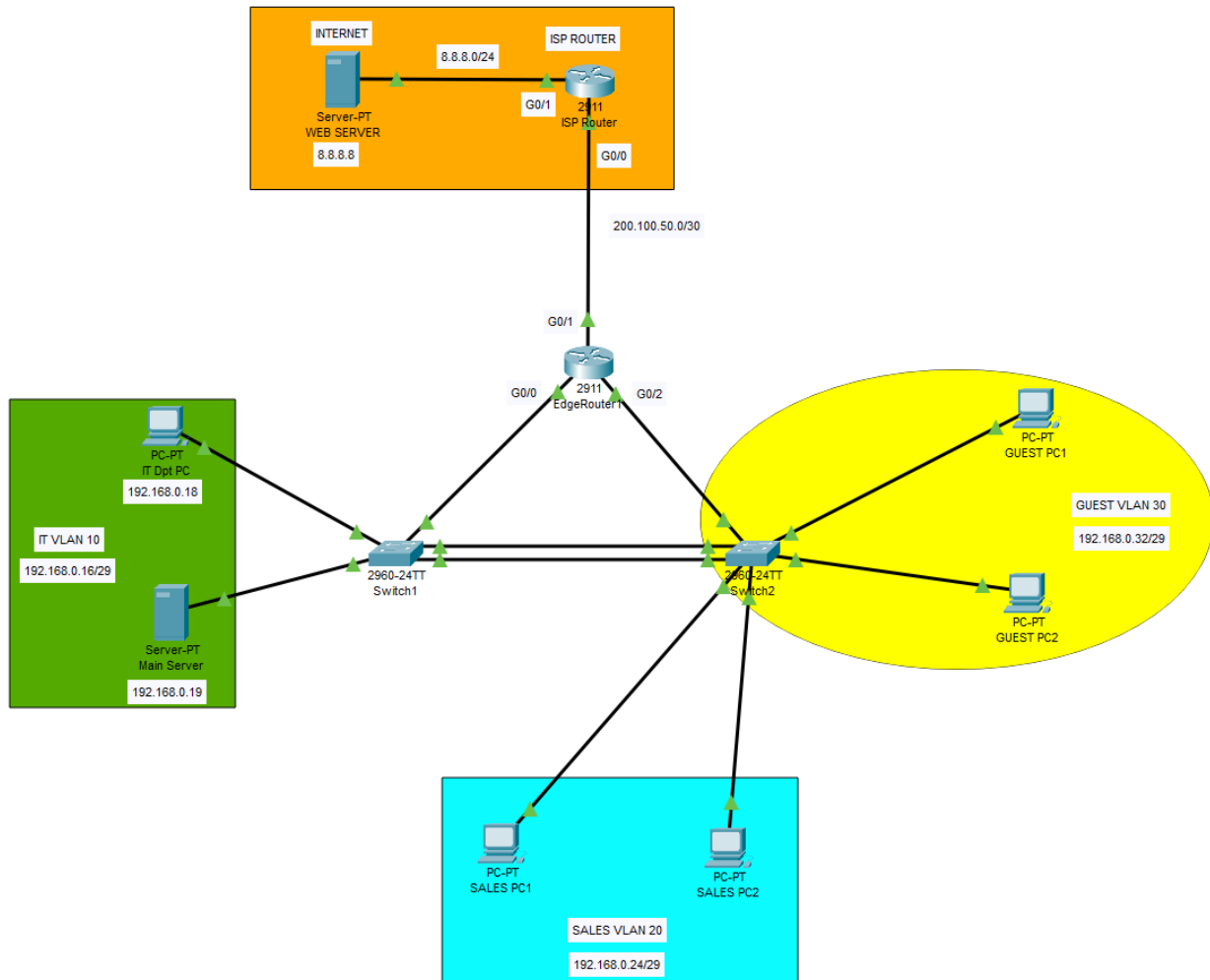
*Describe the **functionality** of the test case in relation to your network project. Identify the relevant tools (devices, subnets, etc.) used in this test case and their specific interactions.*

Port security on the Layer 2 switch connecting Guest VLAN devices was implemented to restrict unauthorized access. It limits the number of allowed MAC addresses per port, ensuring only known guest devices can connect. This prevents unauthorized devices from gaining access to the Guest VLAN, improving network security and maintaining control over endpoint connectivity.

Network Diagram or Segment

*Provide a **network diagram or segment** visualizing the topology and devices used in this test case.*





Testing Method

Summarize the **testing method** used to verify functionality of the network project within the virtual lab environment, including any metrics of success.

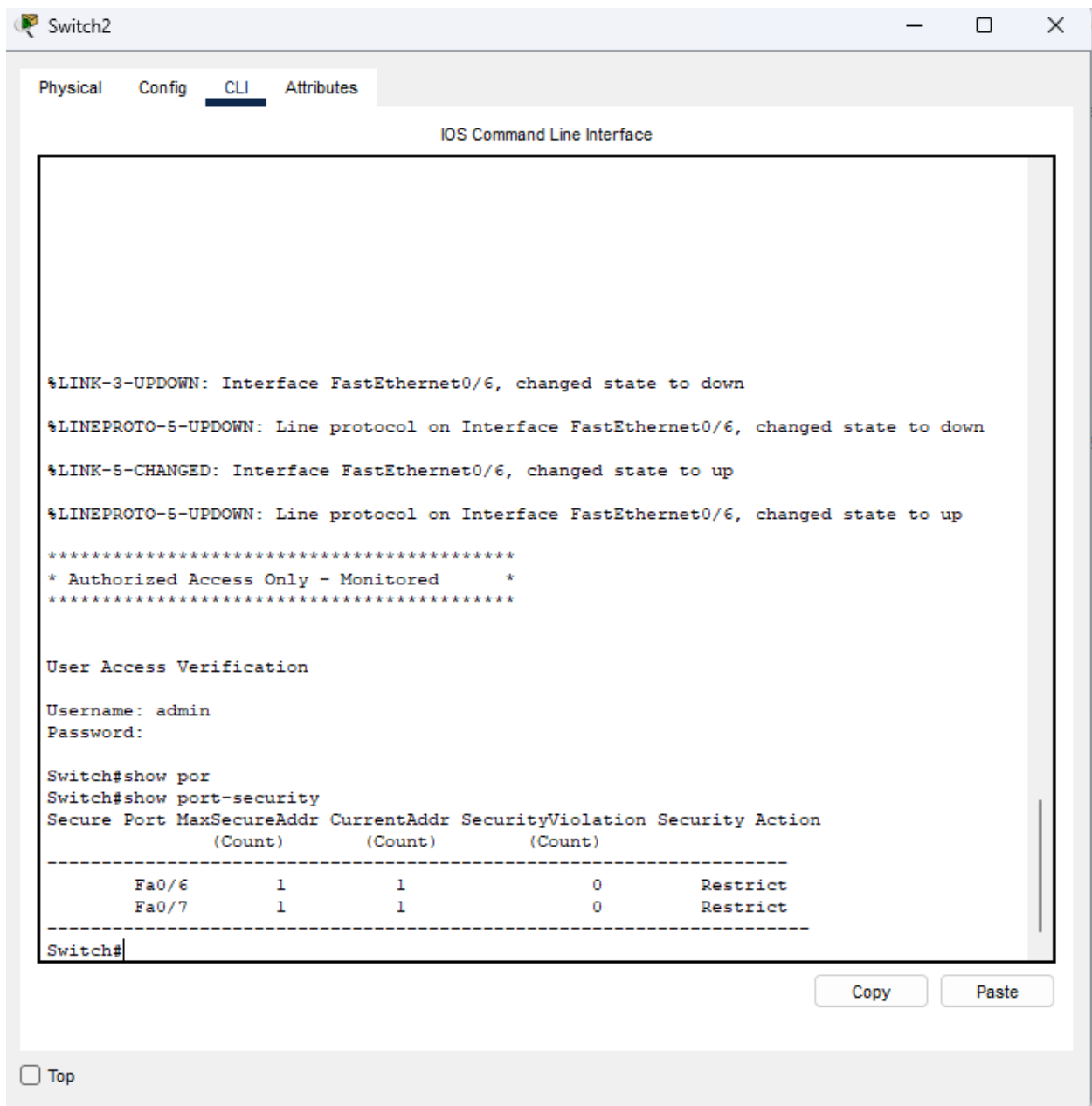
To verify port security, I connected an authorized Guest VLAN device to the secured switch port and confirmed normal network access. Then, I modify the mac address to simulate a second unauthorized device to the same port to test the violation response, ensuring the port went into a restricted state and denied access. Finally, I checked the port security status using the `show port-security` and `show port-security interface` commands to confirm that the allowed MAC address was enforced correctly.



Process List

Provide a comprehensive **process list** of the steps taken within the network project to run the testing method. Include screenshots to illustrate the process and ensure clarity for others attempting to replicate the test.

1. Access Switch2 and verify that port-security is enabled on each port of the Guest VLAN, this case, ports Fa0/6 – 7.
2. Type "show port-security address" to display the sticky MAC addresses learned by the switch.



Switch2

Physical Config **CLI** Attributes

IOS Command Line Interface

```
*****
* Authorized Access Only - Monitored *
*****

User Access Verification

Username:
Username: admin
Password:

Switch#show por
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
              (Count)          (Count)          (Count)
-----
Fa0/6         1             1             0          Restrict
Fa0/7         1             1             0          Restrict
-----

Switch#show port-se
Switch#show port-security add
Switch#show port-security address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
-----
30      00E0.B095.37D6   SecureSticky        Fa0/6    -
30      00E0.F78E.88E3   SecureSticky        Fa0/7    -
-----

Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 1024
Switch#
```

☐ Top

Copy Paste

3. For the functionality test, use port Fa0/6, which has MAC address ending in 37D6.
4. Verify the MAC address by accessing Guest PC1 and confirming it matches.



GUEST PC1

Physical **Config** Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

FastEthernet0

Bluetooth

FastEthernet0

Port Status ☒ On

Bandwidth ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 00E0.B095.37D6

IP Configuration

☒ DHCP

☐ Static

IPv4 Address 192.168.0.35

Subnet Mask 255.255.255.248

IPv6 Configuration

☐ Automatic

☒ Static

IPv6 Address

Link Local Address: FE80::2E0:B0FF:FE95:37D6

☐ Top

5. Modify the MAC address on Guest PC1 to simulate a different endpoint.



GUEST PC1

Physical Config Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

FastEthernet0

Bluetooth

FastEthernet0

Port Status ☒ On

Bandwidth ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 00E0.B095.37D0

IP Configuration

☒ DHCP

☐ Static

IPv4 Address 169.254.55.208

Subnet Mask 255.255.0.0

IPv6 Configuration

☐ Automatic

☒ Static

IPv6 Address

Link Local Address: FE80::2E0:B0FF:FE95:37D6

☐ Top

6. To verify port blocking, confirm that DHCP IP address does not renew.
7. To verify port security violation, access Switch2 and check the port-security address command and confirm that the security violation counter has increased.



Switch2

Physical
Config
CLI
Attributes

IOS Command Line Interface

```

Switch#show port-security address
      Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
      (mins)
-----
30      00E0.B095.37D6    SecureSticky        Fa0/6    -
30      00E0.F78E.88E3    SecureSticky        Fa0/7    -
-----

Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 1024
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
      (Count)          (Count)          (Count)
-----
Fa0/6          1              1              4          Restrict
Fa0/7          1              1              0          Restrict
-----

Switch#show port-security address
      Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
      (mins)
-----
30      00E0.B095.37D6    SecureSticky        Fa0/6    -
30      00E0.F78E.88E3    SecureSticky        Fa0/7    -
-----

Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 1024
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
      (Count)          (Count)          (Count)
-----
Fa0/6          1              1              4          Restrict
Fa0/7          1              1              0          Restrict
-----

Switch#

```

Copy
Paste

☐ Top



Network Troubleshooting

Discuss how you analyzed the network to identify, troubleshoot, and resolve issues during development or when ensuring functionality of the test cases.

One of the problems I had during the project was setting up DHCP. At first it wasn't working, and after some testing, research, and trying different things, I figured out that I needed to add the ip helper-address on the router interfaces to make DHCP work across VLANs. That fixed the issue and let the clients get their IP addresses.

Later on, after I had set up the ACLs to control network access, I noticed the DHCP stopped working again. I had to troubleshoot by looking at how the ACLs were filtering traffic, and found that I needed to add rules to allow UDP traffic for DHCP so that clients could still reach the DHCP server. Once I adjusted the ACLs to allow the proper ports, everything worked fine.

Overall, this troubleshooting showed me how important it is to test every change and check how it affects the rest of the network. Using show commands and checking each step helped me fix the problems and get the network working like I wanted.

