Ministry of Communications
and Information Technology

رواد مصر الرقمية

College Campus Network

Using Cisco Packet Tracer

Presented to DEPI

Track :- cisco cybersecurity engineer

Group :- ONL1_ISS1_S2e

By

Laila Sharkawy

Ashrakat Rashwan

Hager Hamdy

Bassma Abdelaziz

October 2024

Introduction

This project involves the design, implementation, and security of a network infrastructure for a college campus. The campus network must support multiple users, including students, faculty, and administrative staff, while ensuring secure and efficient connectivity across various buildings and departments.

The network design takes into account the need for segmenting different user groups through VLANs, implementing inter-VLAN routing for communication, and securing the network against unauthorized access through features such as Access Control Lists (ACLs) . By using Cisco devices, the project will create a robust and scalable network infrastructure capable of meeting the current and future needs of the college.

The project will be completed in four phases:

1. **Network Design and Configuration**: Developing the network topology and configuring IP addressing and devices.
2. **VLAN and Inter-VLAN Routing**: Setting up VLANs to segment different user groups and configuring inter-VLAN routing for seamless communication.
3. **Network Security Implementation**: Applying security measures such as ACLs, port security, and firewalls to protect sensitive data and ensure network integrity.
4. **Final Testing and Reporting**: Testing the network's functionality, performance, and security, and documenting the results for presentation.

By completing these steps, the project aims to deliver a secure, high-performance network infrastructure that meets the college's operational and security requirements.

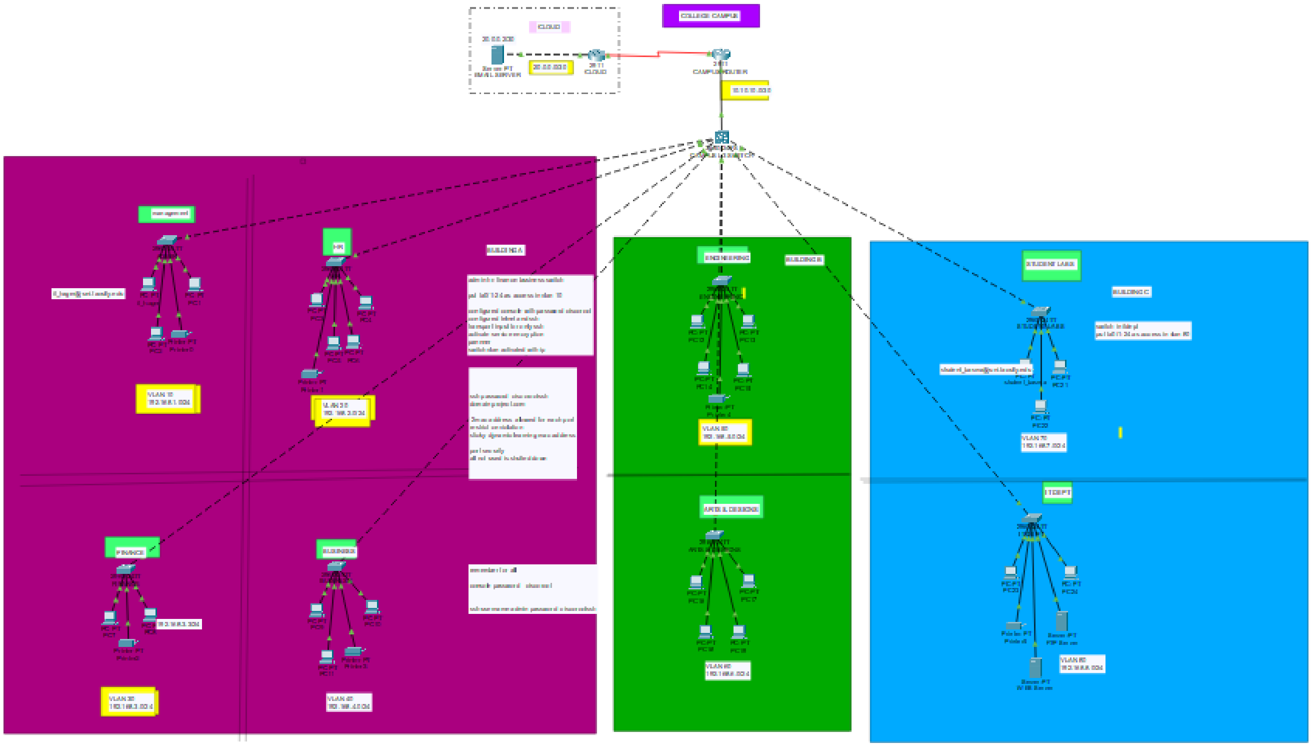
Phase 1 :- Network Design and Configuration

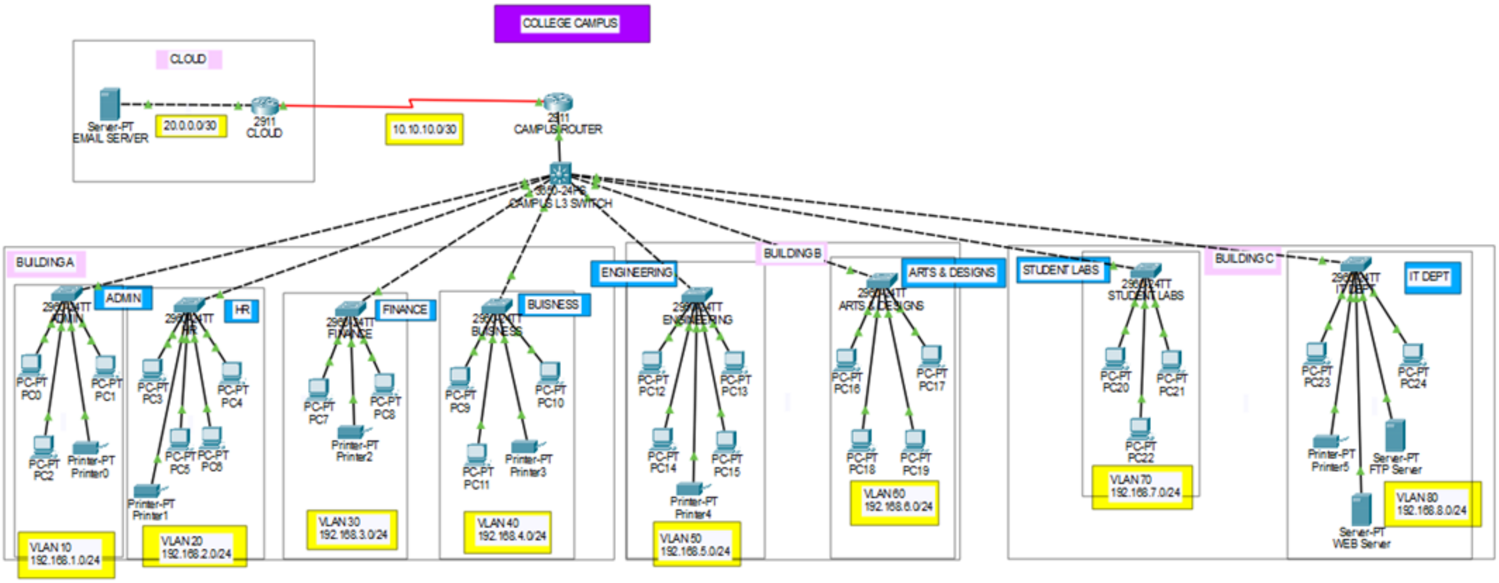
In the first week of the project, the goal was to design a small network for the college campus using Cisco devices. This involved defining the overall network topology, establishing an IP addressing scheme, and configuring the necessary networking devices such as routers and switches.

➢ Network Topology

The network design follows a **hybrid topology**, which combines **star** and **hierarchical** layouts. At the core of the network, a central switch connects to distribution switches, which in turn connect to various VLANs, each representing different segments of the campus (e.g., student network, faculty network, and administrative network).

This topology was chosen for its scalability and ability to segment traffic while maintaining efficient communication between network segments.





➢ IP Addressing Scheme

The IP addressing scheme was implemented to segment each VLAN, with specific subnets assigned to each network segment. DHCP was deployed to simplify IP address management by automatically assigning IP addresses to devices within the network. Each VLAN has its own IP address range.

DHCP Configuration:

The core router was configured with DHCP pools for each VLAN. Devices connected to each VLAN automatically receive an IP address within their respective range, simplifying network management and reducing the risk of IP address conflicts.

VLAN Name	VLAN ID	Subnet (CIDR)	Gateway (Router IP)	DHCP Range
admin	10	192.168.1.0/24	192.168.1.1/24	192.168.1.2-192.168.1.254
hr	20	192.168.2.0/24	192.168.2.1/24	192.168.2.2-192.168.2.254
finance	30	192.168.3.0/24	192.168.3.1/24	192.168.3.2-192.168.3.254
buisness	40	192.168.4.0/24	192.168.4.1/24	192.168.4.2-192.168.4.254
engineering	50	192.168.5.0/24	192.168.5.1/24	192.168.5.2-192.168.5.254
arts	60	192.168.6.0/24	192.168.6.1/24	192.168.6.2-192.168.6.254
studentlabs	70	192.168.7.0/24	192.168.7.1/24	192.168.7.2-192.168.7.254
it	80	192.168.8.0/24	192.168.8.1/24	192.168.8.2-192.168.8.254

DHCP Configuration :-

```
Router(config)#service dhcp
Router(config)#ip dhcp pool admin-pool
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 192.168.1.1
Router(dhcp-config)#ex
```

Device Configuration

The network devices, primarily Cisco routers and switches, were configured with basic settings to ensure connectivity and prepare the infrastructure for VLANs and security settings in later phases. Key configurations include:

- **Router Configuration**:
  - Set up router interfaces and sub-interfaces for each VLAN.
  - Configured routing protocols to manage internal traffic and ensure communication between VLANs.
- **Switch Configuration**:
  - Configured switch ports as access ports for end devices.
  - Configured trunk ports between the switches and the core router to allow VLAN tagging.

Initial configuration scripts for :-

i. CAMPUS ROUTER

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gig0/0
Router(config-if)#no sh

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Router(config-if)#int se0/1/0
Router(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
Router(config-if)#do wr
Building configuration...
[OK]
```

```
Router(config-if)#in se0/1/0
Router(config-if)#clock rate 64000
Router(config-if)#do wr
Building configuration...
[OK]
```

ii. CLOUD

```
Router>EN
Router#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#INT gig0/0
Router(config-if)#no sh

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed
state to up

Router(config-if)#int se0/1/0
Router(config-if)#no sh

Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
Router(config-if)#do wr
Building configuration...
[OK]
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int se0/1/0
Router(config-if)#ip address 10.10.10.2 255.255.255.252
Router(config-if)#ex
Router(config)#do wr
Building configuration...
[OK]

Router(config)#int gig0/0
Router(config-if)#ip address 20.0.0.1 255.255.255.252
Router(config-if)#ex
Router(config)#ip route 192.168.1.0 255.255.255.0 se0/1/0
%Default route without gateway, if not a point-to-point interface, may impact
performance
```

Phase 2 :- VLANs and Inter-VLAN Routing

In phase 2, the focus was on implementing VLANs to segment the network and setting up Inter-VLAN routing. This was done to ensure that traffic from different segments (students, faculty, and administration) could be isolated, while still allowing controlled communication between them when necessary. VLAN trunks were also configured to enable multiple VLANs to be carried across the same physical links between switches and routers.

➢ VLAN Implementation

Each department and group within the campus was assigned to a dedicated VLAN, improving both network performance and security.

▪ VLAN configuration scripts:-

iii. For each switch (taking into account the VLANs differing)

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range fa0/1-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
Switch(config-if-range)#do wr
```

➢ Inter-VLAN Routing

To allow communication between VLANs, **Router-on-a-Stick** was configured on the core router. Each VLAN was assigned to a sub-interface on the router, which enabled it to route traffic between VLANs through a single physical interface.

Inter-VLAN routing documentation:-

iv. CAMPUS ROUTER

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gig0/0.10
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10,
changed state to up

Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#ex
Router(config)#int gig0/0.20
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20,
changed state to up

Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#ex
```

- **the same applies to the rest of the VLANs**

VLAN Trunk Configuration

Trunk links were set up between switches and the core router to carry traffic for multiple VLANs over a single physical connection. This was achieved by configuring the switch port as trunk port.

VLAN Trunk Configuration :-

v. L3 SWITCH

```
Switch(config)#int g1/0/1
Switch(config-if)#sw
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1,
changed state to up

Switch(config-if)#no shut
Switch(config-if)#exit
```

Phase 3 :- Network Security Implementation

In phase 3, the objective was to secure the network by implementing various security features, such as port security, and Access Control Lists (ACLs). These security measures aimed to protect the network from unauthorized access and ensure that only permitted traffic could flow between VLANs

➢ Security Features Implemented

a) Port Security

Configured on switches to limit the number of devices that can connect to each port. This feature restricts access to the network and helps prevent MAC address spoofing.

▪ Port security Configuration :-

```
s-engineering(config)#interface range fa0/1-24
s-engineering(config-if-range)#switchport mode access
s-engineering(config-if-range)#switchport port-security maximum 2
s-engineering(config-if-range)#switchport port-security violation restrict
s-engineering(config-if-range)#switchport port-security mac-address sticky
s-engineering(config-if-range)#exit
```

b) Access Control Lists (ACLs)

Configured on the router to control the flow of traffic between VLANs. ACLs were used to permit or deny specific traffic based on IP addresses, protocols, and ports.

ACL Configuration :-

```
r-basic(config)#access-list 120 deny tcp any 192.168.8.0 0.0.0.255 eq 21

r-basic(config)#access-list 120 deny tcp any 192.168.8.0 0.0.0.255 eq 20

r-basic(config)#access-list 120 permit tcp any any eq 80

r-basic(config)#access-list 120 permit tcp any any eq 443

r-basic(config)#access-list 120 permit ip any any

r-basic(config)#interface gigabitEthernet 0/0.80

r-basic(config-subif)#ip access-group 120 in
```

Security Best Practices

The security configuration followed industry best practices, including:

- **Disabling unused ports** on switches and placing them in an unused VLAN to prevent unauthorized access.
- **Enabling SSH** on all switches to ensure secure remote management.

SSH Configuration :-

```
s-engineering(config)#ip domain-name project.com

s-engineering(config)#crypto key generate rsa

The name for the keys will be: s-engineering.project.com

Choose the size of the key modulus in the range of 360 to 4096 for your

  General Purpose Keys. Choosing a key modulus greater than 512 may take

  a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

*Mar 2 1:19:49.895: %SSH-5-ENABLED: SSH 1.99 has been enabled

s-engineering(config)#ip ssh version 2

s-engineering(config)#line vty 0 4
```

```
s-engineering(config-line)#login local

s-engineering(config-line)#transport input ssh

s-engineering(config-line)#exit

s-engineering(config)#username admin secret ciscorootssh
```

- **Using strong password policies** and limiting administrative access via ACLs.

Configuring Console Access :-

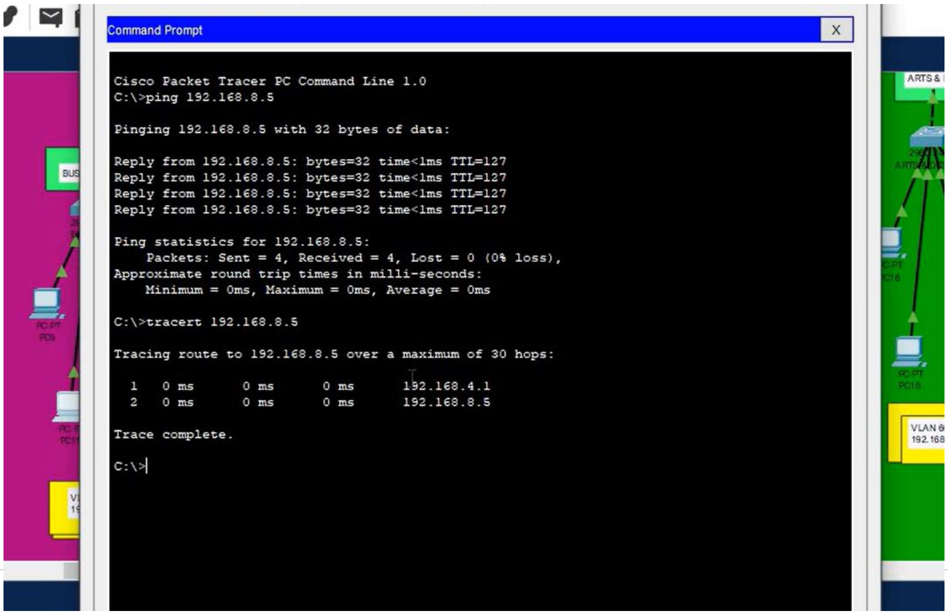
```
s-engineering(config)#line console 0

s-engineering(config-line)#password ciscoroot

s-engineering(config-line)#login

s-engineering(config-line)#exit
```

Phase 4 :- Final Testing and Reporting

In Week 4, the final phase of the project, extensive testing was performed to validate network functionality, performance, and security. Testing tools such as ping, traceroute, and vulnerability scanners were used to ensure that the network met design requirements and was free from security vulnerabilities.

Network Testing

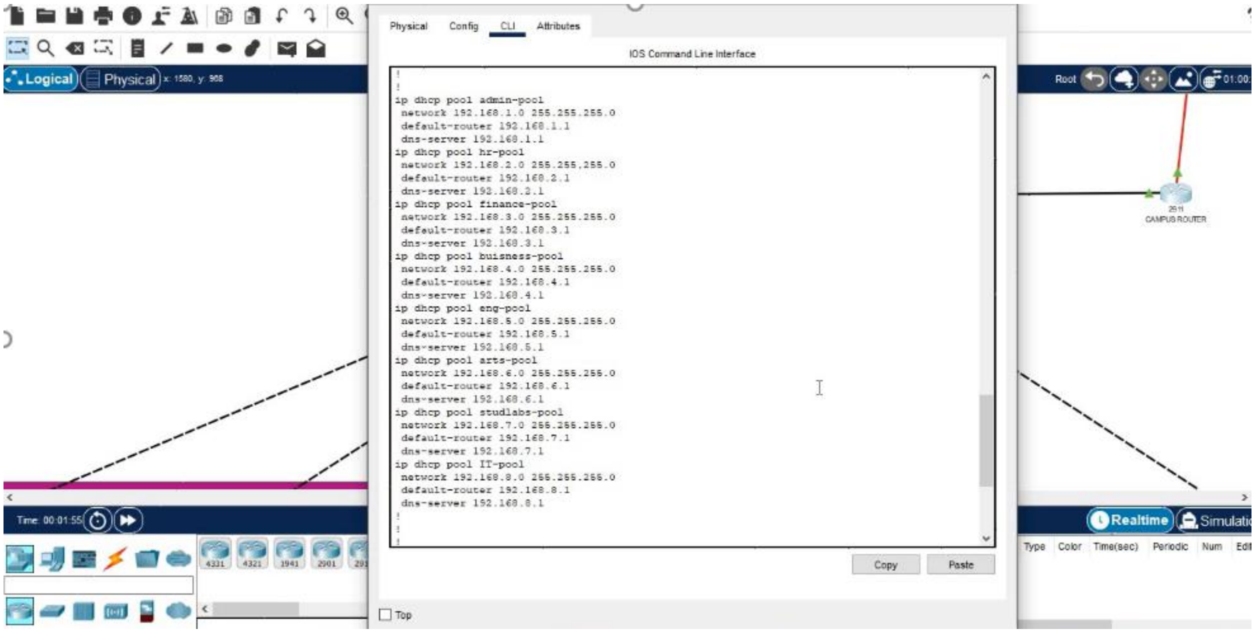
- **Ping and Connectivity Tests**: Ping tests were performed between devices in different VLANs to verify that inter-VLAN routing was working correctly. Connectivity between internal devices and external networks was also tested.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.8.5

Pinging 192.168.8.5 with 32 bytes of data:

Reply from 192.168.8.5: bytes=32 time<1ms TTL=127
Reply from 192.168.8.5: bytes=32 time<1ms TTL=127
Reply from 192.168.8.5: bytes=32 time<1ms TTL=127
Reply from 192.168.8.5: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.8.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>tracert 192.168.8.5

Tracing route to 192.168.8.5 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.4.1
  2   0 ms      0 ms      0 ms      192.168.8.5

Trace complete.

C:\>
```

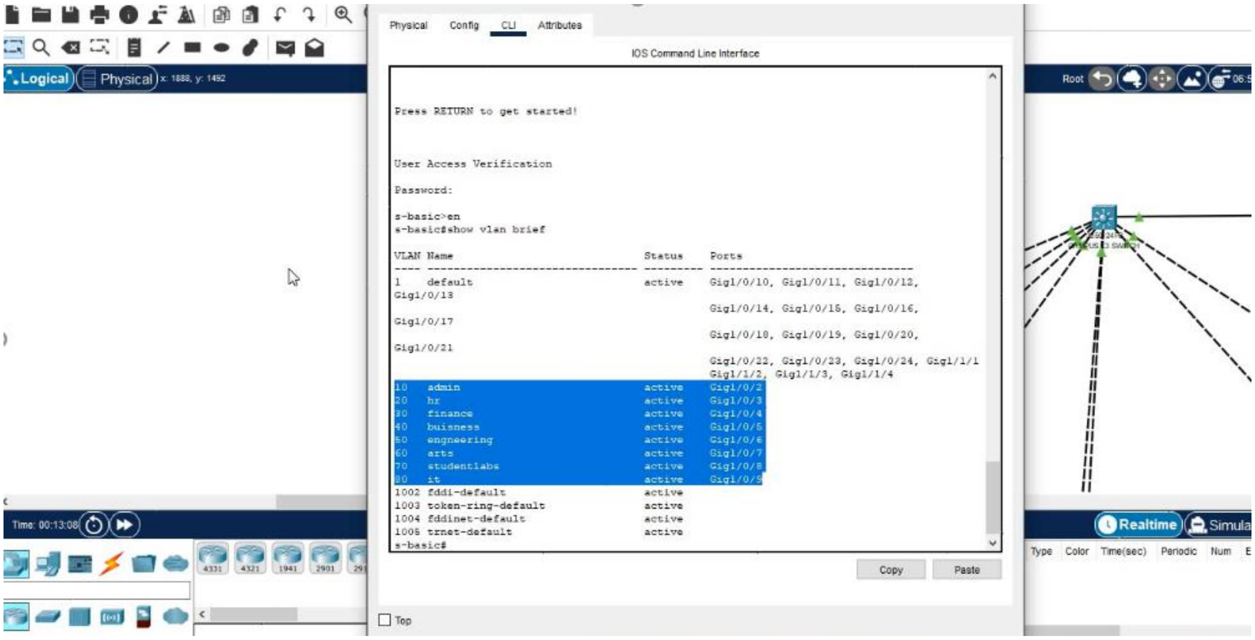
- **Performance Testing**: We monitored network throughput and latency to ensure that the network provided adequate bandwidth and low latency for different departments.

IP address configuration using DHCP



```
!
!
ip dhcp pool admin-pool
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 192.168.1.1
ip dhcp pool hr-pool
 network 192.168.2.0 255.255,255.0
 default-router 192.168.2.1
 dns-server 192.168.2.1
ip dhcp pool finance-pool
 network 192.168.3.0 255.255.255.0
 default-router 192.168.3.1
 dns-server 192.168.3.1
ip dhcp pool buisness-pool
 network 192.168.4.0 255.255.255.0
 default-router 192.168.4.1
 dns-server 192.168.4.1
ip dhcp pool eng-pool
 network 192.168.5.0 255.255.255.0
 default-router 192.168.5.1
 dns-server 192.168.5.1
ip dhcp pool arts-pool
 network 192.168.6.0 255.255.255.0
 default-router 192.168.6.1
 dns-server 192.168.6.1
ip dhcp pool studlabs-pool
 network 192.168.7.0 255.255.255.0
 default-router 192.168.7.1
 dns-server 192.168.7.1
ip dhcp pool IT-pool
 network 192.168.8.0 255.255.255.0
 default-router 192.168.8.1
 dns-server 192.168.8.1
!
!
!
```

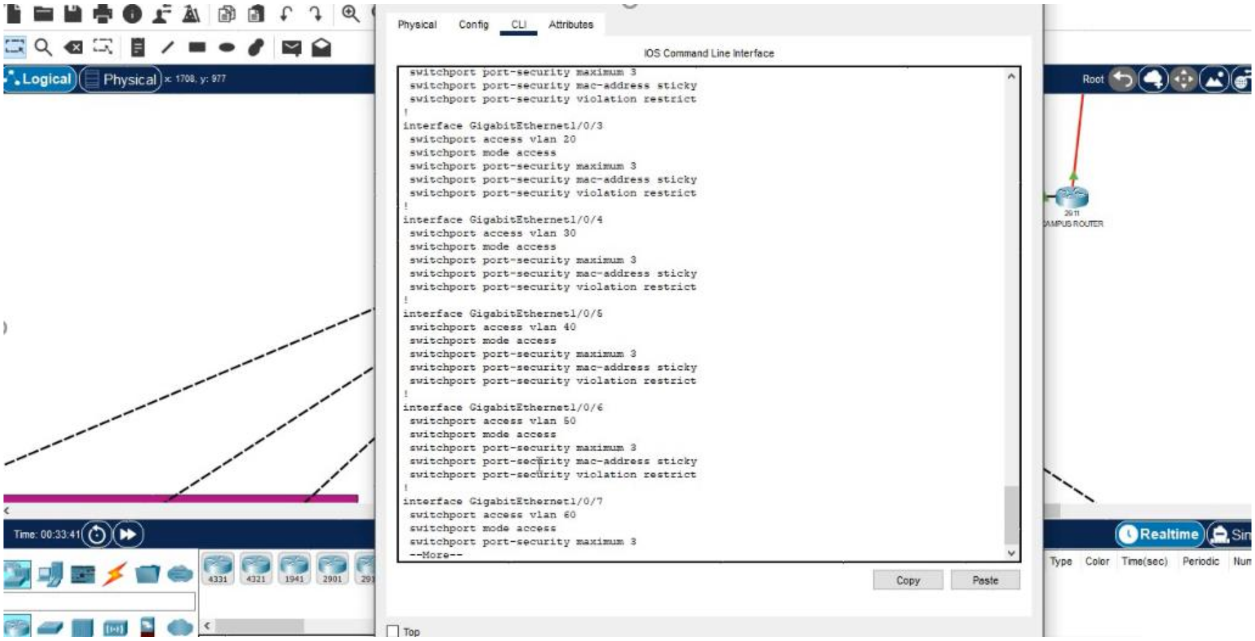
VLANS Configuration



```
Press RETURN to get started!



User Access Verification

Password:

s-basic>en
s-basic#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/10, Gig1/0/11, Gig1/0/12,
Gig1/0/13
                                                Gig1/0/14, Gig1/0/15, Gig1/0/16,
Gig1/0/17
                                                Gig1/0/18, Gig1/0/19, Gig1/0/20,
Gig1/0/21
                                                Gig1/0/22, Gig1/0/23, Gig1/0/24, Gig1/1/1
                                                Gig1/1/2, Gig1/1/3, Gig1/1/4
10   admin                            active    Gig1/0/2
20   hr                               active    Gig1/0/3
30   finance                          active    Gig1/0/4
40   buisness                         active    Gig1/0/5
50   engneering                       active    Gig1/0/6
60   arts                             active    Gig1/0/7
70   studentlabs                      active    Gig1/0/8
80   it                               active    Gig1/0/9
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
s-basic#
```

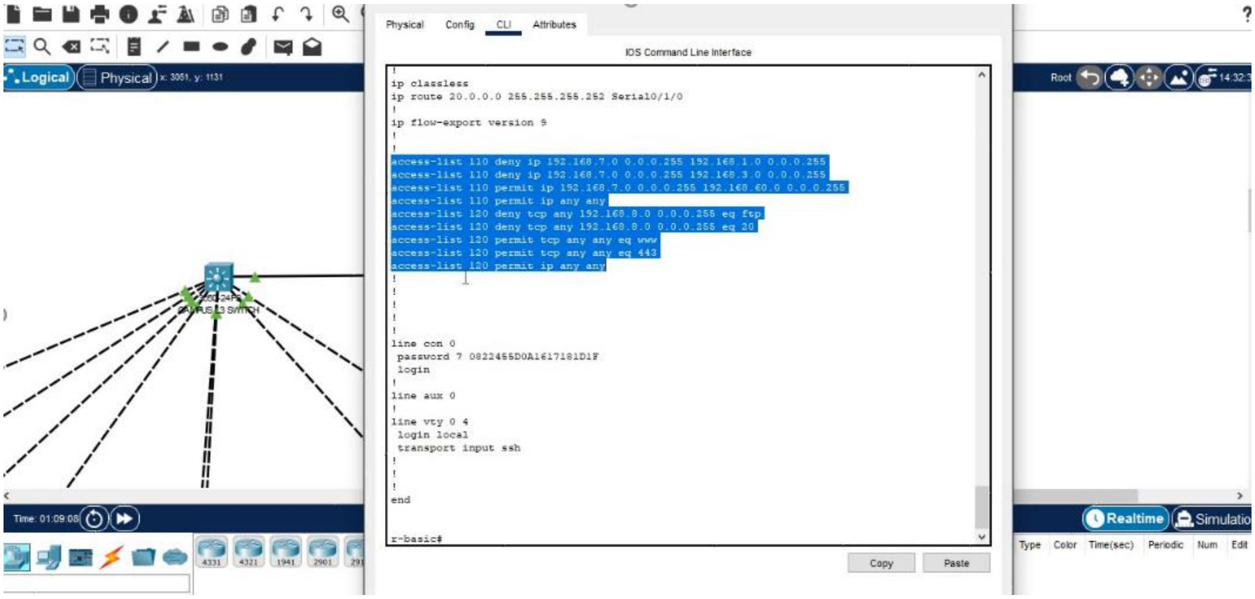
- **Vulnerability Scanning**: The network was scanned for security vulnerabilities, and any identified issues were addressed immediately by modifying ACLs .

  - Port Security Configuration on Campus L3 Switch



```
 switchport port-security maximum 3
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
interface GigabitEthernet1/0/3
 switchport access vlan 20
 switchport mode access
 switchport port-security maximum 3
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
interface GigabitEthernet1/0/4
 switchport access vlan 30
 switchport mode access
 switchport port-security maximum 3
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
interface GigabitEthernet1/0/5
 switchport access vlan 40
 switchport mode access
 switchport port-security maximum 3
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
interface GigabitEthernet1/0/6
 switchport access vlan 50
 switchport mode access
 switchport port-security maximum 3
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
interface GigabitEthernet1/0/7
 switchport access vlan 60
 switchport mode access
 switchport port-security maximum 3
 --More--
```

  - ACL Configuration



```
!
ip classless
ip route 20.0.0.0 255.255.255.252 Serial0/1/0
!
ip flow-export version 9
!
!
access-list 110 deny ip 192.168.7.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 110 deny ip 192.168.7.0 0.0.0.255 192.168.3.0 0.0.0.255
access-list 110 permit ip 192.168.7.0 0.0.0.255 192.168.60.0 0.0.0.255
access-list 110 permit ip any any
access-list 120 deny tcp any 192.168.8.0 0.0.0.255 eq ftp
access-list 120 deny tcp any 192.168.8.0 0.0.0.255 eq 20
access-list 120 permit tcp any any eq www
access-list 120 permit tcp any any eq 443
access-list 120 permit ip any any
!
!
!
!
!
line con 0
 password 7 0822455D0A1617181D1F
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
!
!
!
end


r-basic#
```

➢ Results

The tests showed that the network functioned as expected, with strong connectivity between VLANs and no significant performance issues. All unauthorized access attempts were successfully blocked by the ACLs .