Project Report
On
Computer Networking: Concepts
(CSE3751)

[Smart Office Network with Inter-VLAN Routing, STP, and Access Control]

Submitted by:

Name1: Ashutosh Raj **Regd. No.:**2241018015
Name2: Dinanath Dash **Regd. No.:**2241004161
Name3: Swarnabha Roy **Regd. No.:**2241018192
Name4: Pikesh Yadav **Regd. No.:** 2241025009

B. Tech. CSE 5th Semester (Section 2241026)

INSTITUTE OF TECHNICAL EDUCATION AND RESEARCH
(FACULTY OF ENGINEERING)
SIKSHA 'O' ANUSANDHAN (DEEMED TO BE UNIVERSITY),
BHUBANESWAR, ODISHA

Declaration

We, the undersigned students of B. Tech. of **CSE** Department hereby declare that we own the full responsibility for the information, results etc. provided in this PROJECT titled **"Smart Office Network with Inter-VLAN Routing, STP, and Access Control"** submitted to **Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar** for the partial fulfillment of the subject **Computer Networking: Concepts (CSE 3751)**. We have taken care in all respect to honor the intellectual property right and have acknowledged the contribution of others for using them in academic purpose and further declare that in case of any violation of intellectual property right or copyright we, as the candidate(s), will be fully responsible for the same.

Name1: Ashutosh Raj Regd. No.:2241018015

Name2: Dinanath Dash Regd. No.:2241004161

Name3: Swarnabha Roy Regd. No.:2241018192

Name4: Pikesh Yadav Regd. No.:2241025009

Date:07-01-2025

Place: Bhubaneswar

Abstract

The design of a smart office network focuses on creating a secure, efficient, and reliable communication system that supports a variety of devices, workstations, and administrative servers. This network will be segmented into various Virtual Local Area Networks (VLANs) to ensure logical grouping and better traffic management. This network design will be tested through various scenarios to ensure its robustness, including STP failover testing, ACL-based access control, and the verification of inter-VLAN communication.

The smart office network is composed of a variety of devices, including workstations and administrative servers. The network will be designed with the following components:

1. **VLANs**: Devices will be logically grouped into VLANs, ensuring effective communication while minimizing broadcast traffic.
2. **Inter-VLAN Routing**: A router will be used to enable communication between VLANs facilitating seamless data flow across VLAN boundaries.
3. **Spanning Tree Protocol (STP)**: STP will be implemented to prevent network loops, ensuring reliable network operation. One of the switch will be elected as the root bridge for optimal routing.
4. **Access Control Lists (ACLs)**: ACLs will be configured to limit access to the administrative servers, ensuring that only authorized devices within the network can access critical resources.

Contents

1.Introduction

The office network is segmented into 3 Virtual Local Area Networks (VLANs), (VLAN 10, VLAN 20, VLAN 30) with Network ID: 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24 and Gateway: 192.168.10.1, 192.168.20.1, 192.168.30.1 respectively, which logically separate devices into different groups. One of the VLAN consists of Server, and other two consists of 6 devices connected through switches and a router.
VLAN 10: PC1, PC2, PC5, PC6
VLAN 20: PC0, Device (Laptop)
VLAN 30: SERVER

This segmentation improves network efficiency by reducing broadcast traffic and enhancing security by isolating sensitive information within specific VLANs. However, to ensure communication between these separate VLANs, Inter-VLAN Routing is implemented, allowing devices from different VLANs to communicate securely and efficiently.

Network redundancy is another crucial aspect of this design, which is addressed using the Spanning Tree Protocol (STP). The root bridge election process will designate a central switch, Switch 0 as the most reliable and authoritative device in the network. By applying strict Access Control Lists (ACLs) rules, only authorized devices that is PC1 and Device will be able to access the server, ensuring sensitive data and network resources remain protected. The proposed network setup is tested through various scenarios to verify its effectiveness in maintaining communication, redundancy, and security.

2.Problem Statement

Objective: Design and configure a smart office network using Inter-VLAN Routing and Spanning Tree Protocol (STP) to provide secure and reliable communication between VLANs. Additionally, implement Access Control Lists (ACLs) to restrict server access to authorized devices only.

1. **VLANs** segregate devices into logical groups.

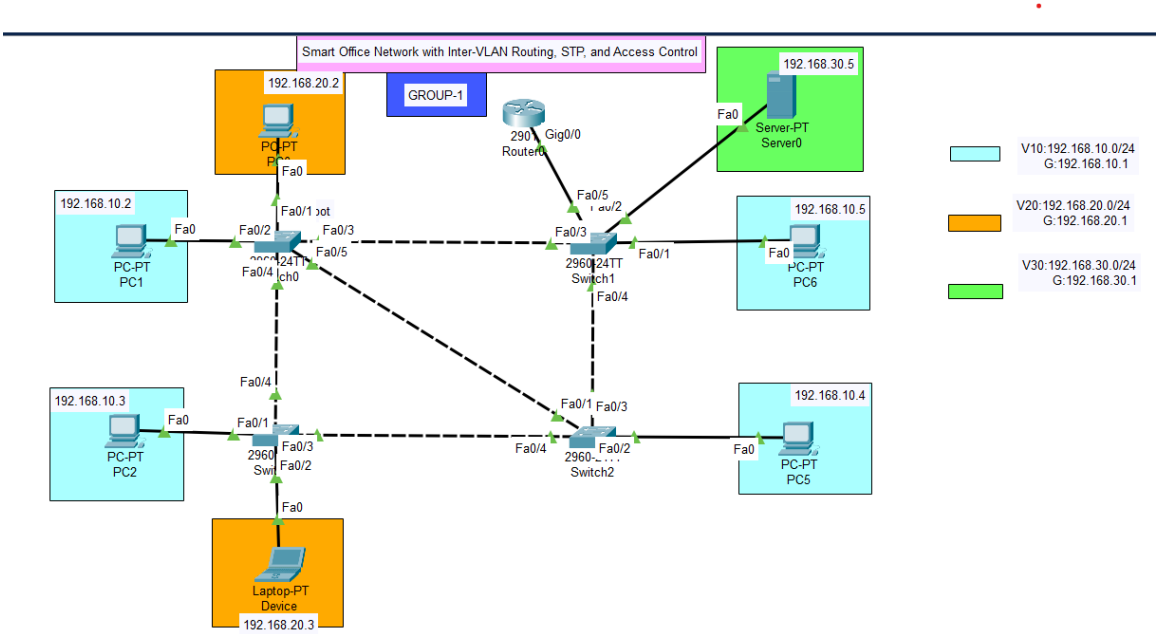
2**. Inter-VLAN Routing** enables communication between these groups

3. **STP** ensures redundancy and prevents loops while electing a switch connected to the administrative servers as the root bridge.

4**. Access Control Lists (ACLs)** restrict access to the administrative servers, allowing only authorized devices.

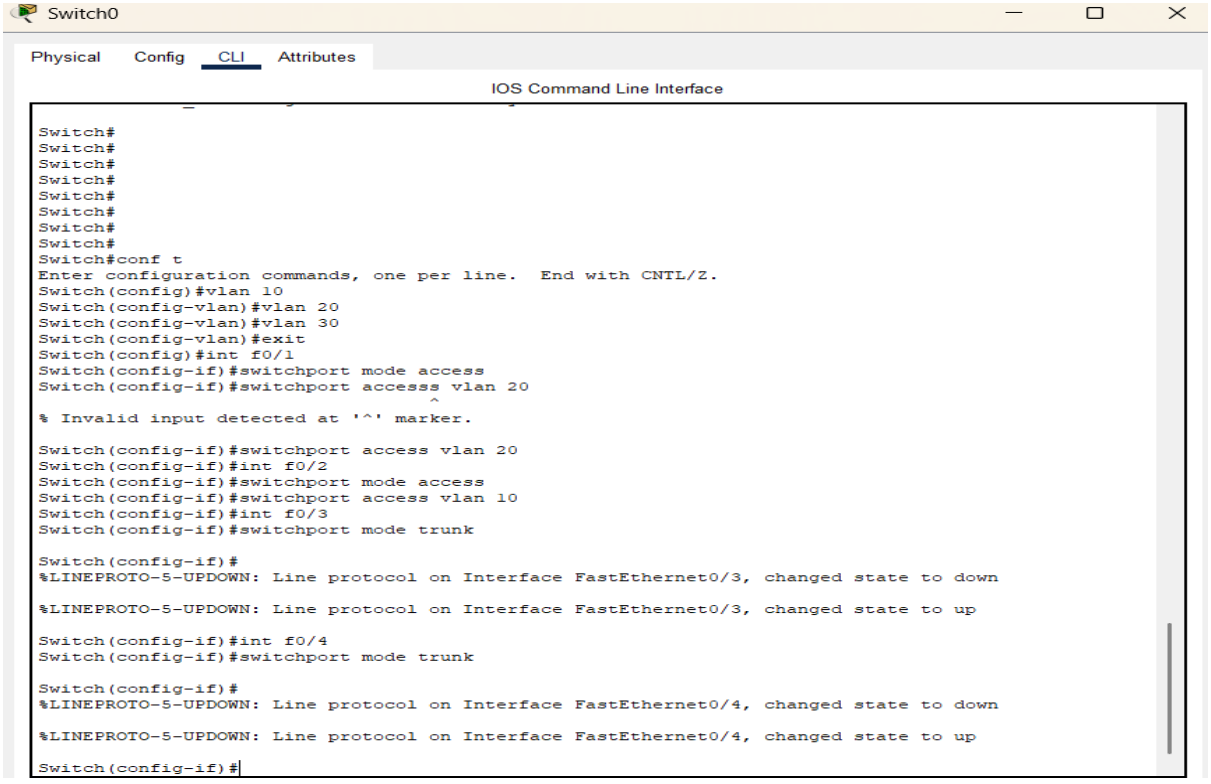
3.Methodology

I. Designing the Topology

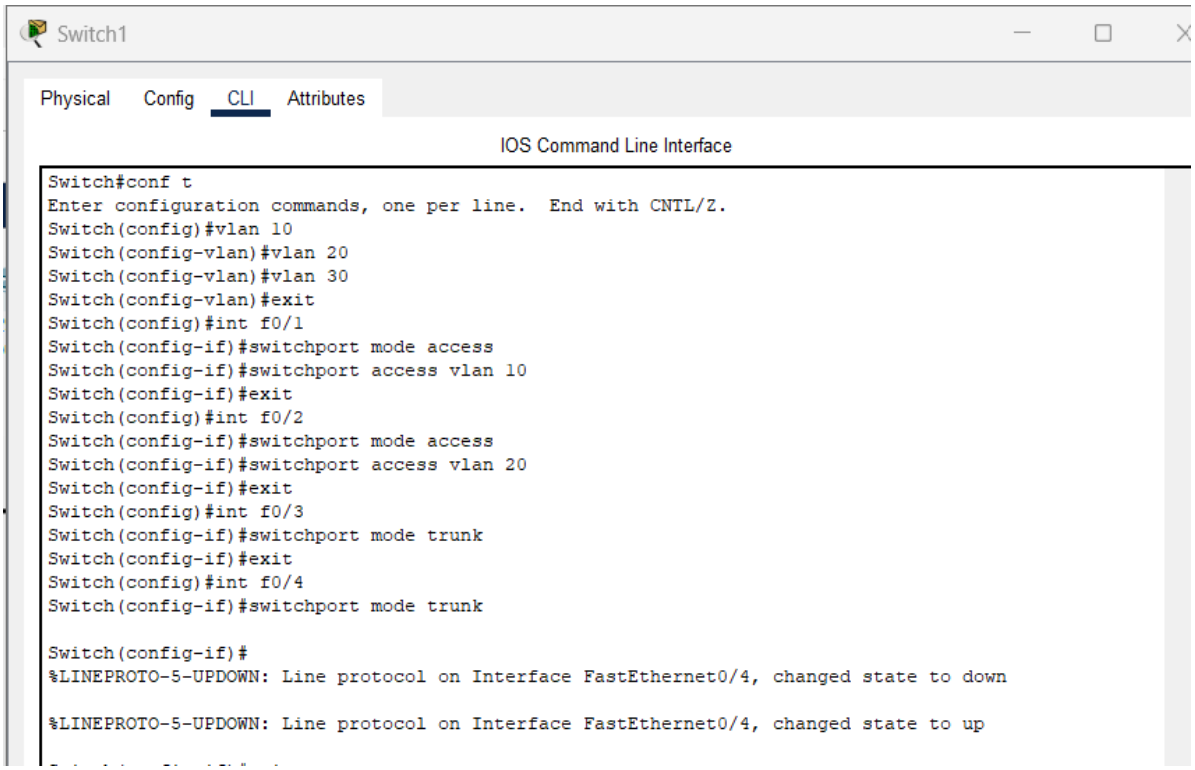


II. Configuring the devices.

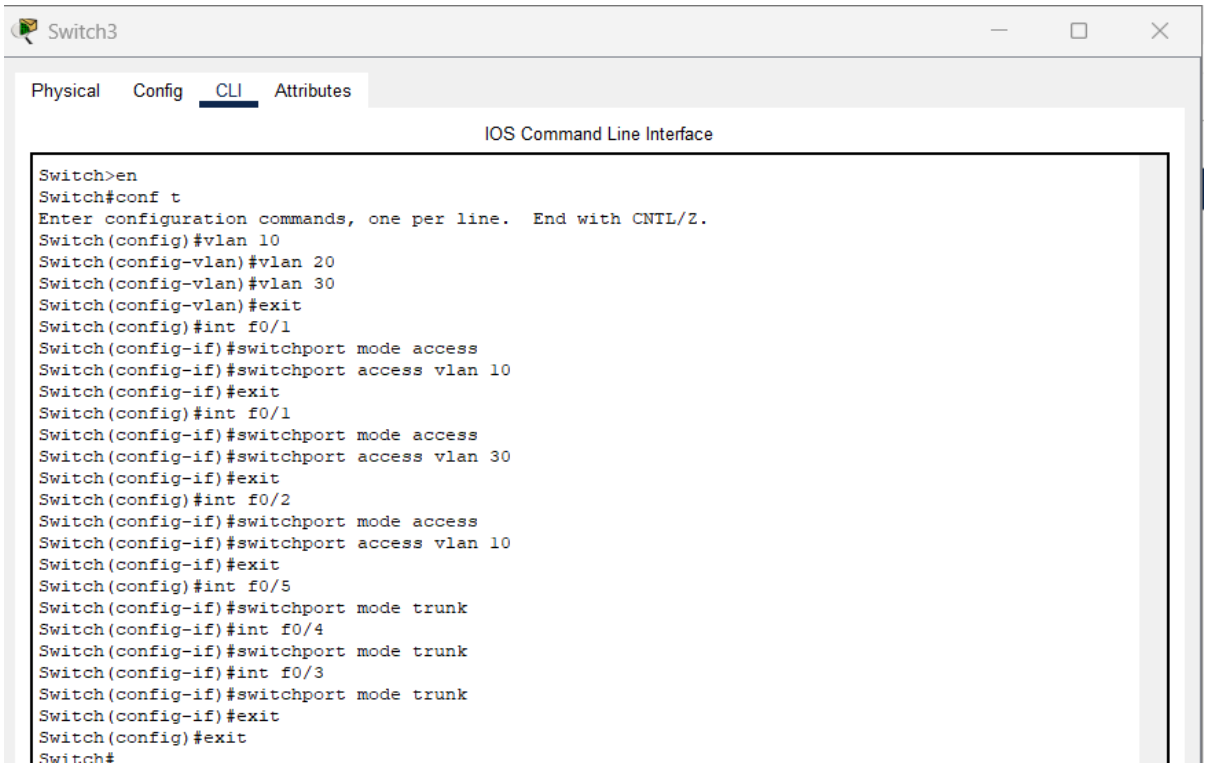
❖ Configuring Switch1



❖ Configuring Switch2



❖ Configuring Switch4



III. CLI instructions to attend the required objective.

a) VLAN Creation: - vlan 10/20/30

Purpose: Creates VLANs and assigns descriptive names.

Example: vlan 10 creates VLAN 10

b) Assign Access Ports to VLANs: -

```
interface FastEthernet0/1
switchport mode access
switchport access vlan 10
```

Purpose: Sets the interface as an access port**.**

Assigns it to VLAN 10. Similar configuration applies for VLAN 20 and VLAN 30

c) Configure Trunk Port: -

```
interface FastEthernet0/1
switchport mode trunk
```

Purpose: Configures the port as a trunk link (used to carry multiple VLANs). Allows only VLANs 10, 20, and 30 to traverse this trunk.

d) Verify STP Configuration: - show spanning-tree

Purpose: To verify the root bridge election, confirm the STP topology, and ensure proper redundancy and loop prevention in the network.

e) Create Sub-Interfaces for Inter-VLAN Routing:

```
Interface GibabitEthernal0/1.10
Encapsulation dot 10
ip address 192.168.10.1 255.255.255.0
```

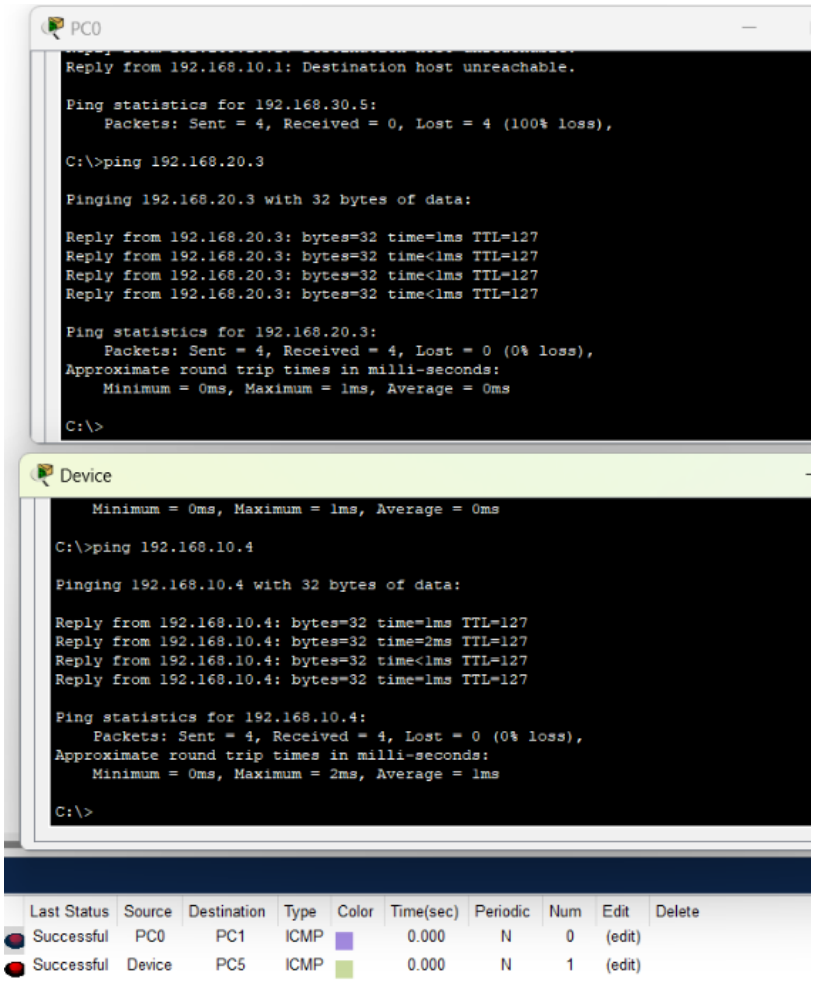
Purpose: To configure a sub-interface on the router for VLAN 10, enabling Inter-VLAN Routing with Ip address 192.168.10.1 as the gateway for devices in VLAN 10.

f) Configure Access Control List (ACL): -

```
access-list 100 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
```

Purpose: To permit traffic between specific source and destination subnets, deny all other traffic to the 192.168.30.0/24 subnet, and allow all other traffic.

4.Results & Interpretation



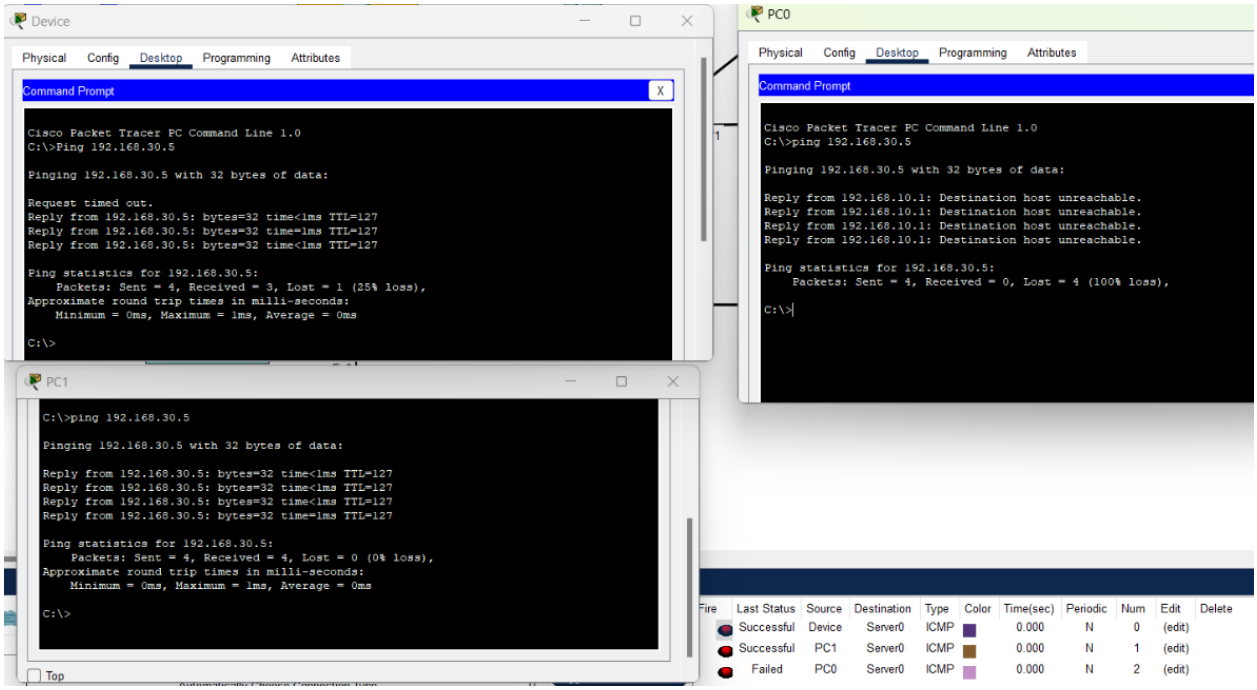
Above image shows Inter-VLAN communication using ping command between:

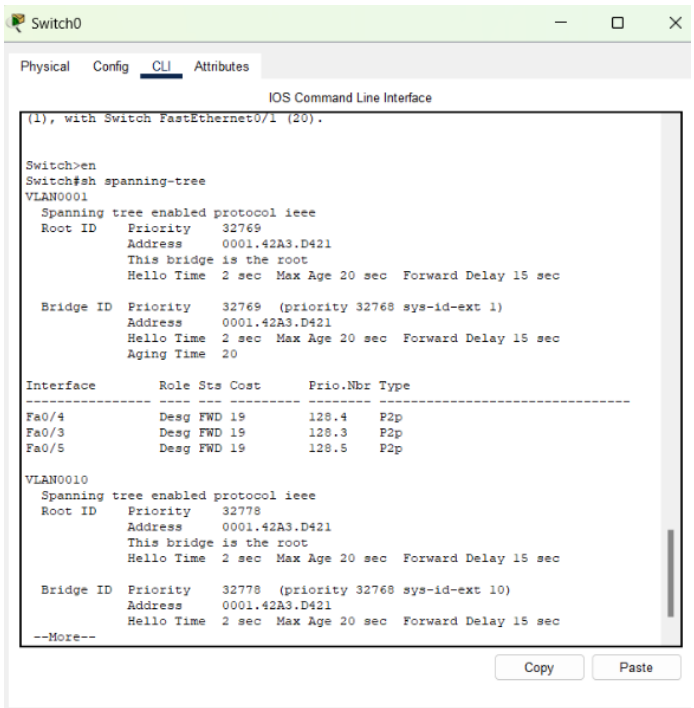
1. PC0 of VLAN 10 and PC1 of VLAN 20.
2. Device of VLAN 20 PC5 of VLAN 10.

Below image shows access-list and ACL using ping command:

1. Device and PC1 can access Server because they are there in access-list.
2. All other PCs (Here, PC0) cannot access Server because they are not in access-list.

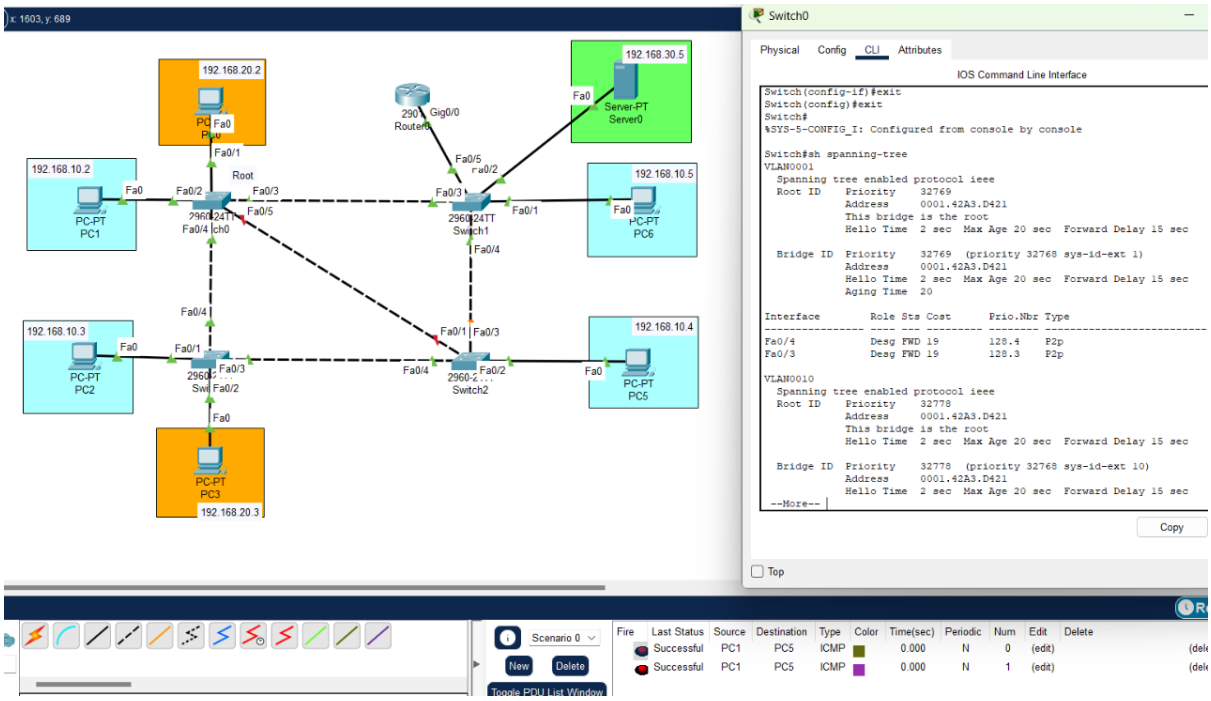
```
Router(config)#access-list 100 permit ip 192.168.20.2 0.0.0.255 host 192.168.30.5
Router(config)#access-list 100 permit ip 192.168.20.3 0.0.0.255 host 192.168.30.5
Router(config)#access-list 100 deny ip any host 192.168.30.0
Router(config)#int g0/0.30
Router(config-subif)#ip access-group 100 out
Router(config-subif)#exit
```

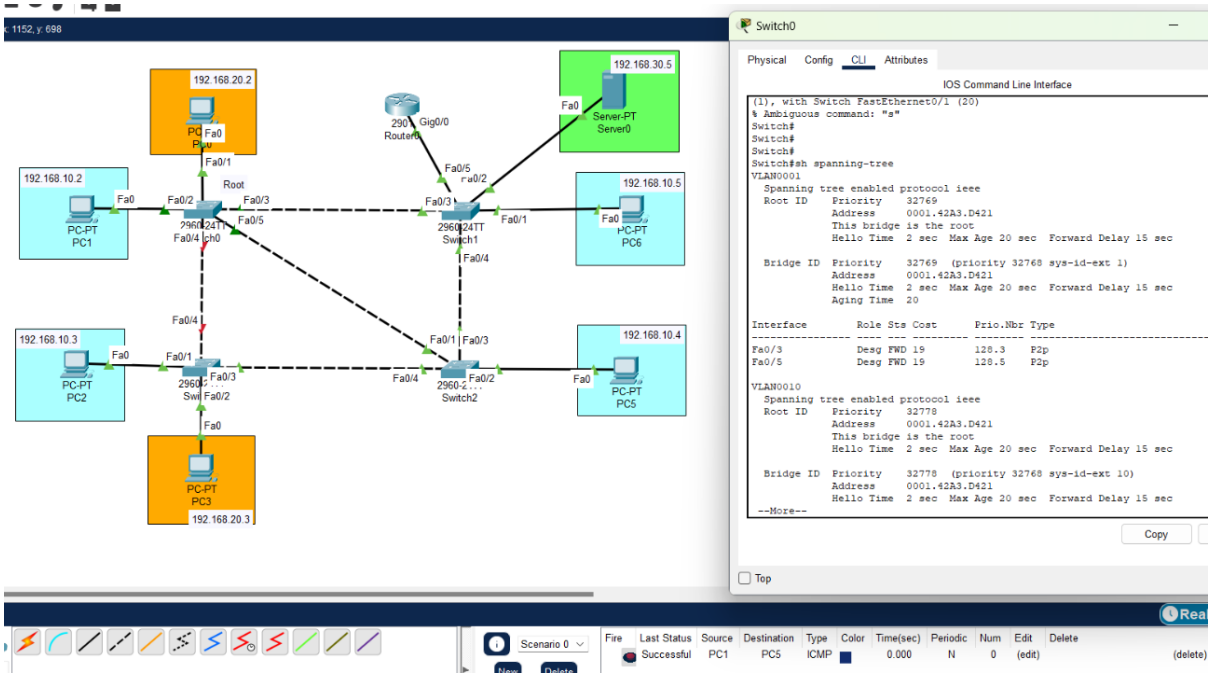




Above image shows Switch0 spanning-tree, where it is mentioned: ‘This bridge is the root’.

Below images show STP: Redundant link is disabled to observe failover and verify S1 remains the root bridge.


Switch0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#sh spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 0001.42A3.D421
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0001.42A3.D421
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20
Interface Role Sts Cost Prio.Nbr Type
Fa0/4 Desg FWD 19 128.4 P2p
Fa0/3 Desg FWD 19 128.3 P2p
VLAN0010
Spanning tree enabled protocol ieee
Root ID Priority 32778
Address 0001.42A3.D421
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
Address 0001.42A3.D421
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
--More--
Copy
Top
192.168.20.2
192.168.30.5
192.168.10.2
192.168.10.5
192.168.10.3
192.168.10.4
192.168.20.3
PC-PT PC1
PC-PT PC2
PC-PT PC3
PC-PT PC5
PC-PT PC6
Server-PT Server0
Root
Switch1
Switch2
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
Successful PC1 PC5 ICMP 0.000 N 0 (edit)
Successful PC1 PC5 ICMP 0.000 N 1 (edit)


Switch0
Physical
Config
CLI
Attributes
IOS Command Line Interface
(1), with Switch FastEthernet0/1 (20)
% Ambiguous command: "s"
Switch#
Switch#
Switch#sh spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 0001.42A3.D421
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0001.42A3.D421
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
Fa0/5 Desg FWD 19 128.5 P2p
VLAN0010
Spanning tree enabled protocol ieee
Root ID Priority 32778
Address 0001.42A3.D421
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
Address 0001.42A3.D421
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
--More--
Copy
Top
192.168.20.2
192.168.30.5
192.168.10.2
192.168.10.5
192.168.10.3
192.168.10.4
192.168.20.3
PC-PT PC1
PC-PT PC2
PC-PT PC3
PC-PT PC5
PC-PT PC6
Server-PT Server0
Root
Switch1
Switch2
Scenario 0
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
Successful PC1 PC5 ICMP 0.000 N 0 (edit)

5.Conclusion

In this project, we've successfully designed and set up a smart office network that addresses important needs like efficiency, security, and reliability. By dividing the network into VLANs, we've created a more organized and secure environment where different groups of devices can communicate without overwhelming the network. Inter-VLAN Routing ensures that devices in different VLANs can still talk to each other when needed.

To prevent network issues like loops, we used Spanning Tree Protocol (STP). STP makes sure that if one path fails, another can take over, keeping the network up and running smoothly. Switch0 was set as the root bridge, ensuring that the network always stay connected.

Security was also a top priority. Access Control Lists (ACLs) were set up to restrict access to sensitive resources, such as the administrative servers. Only authorized devices can reach these servers, preventing unauthorized access and enhancing the network's safety.

All the commands were provided through CLI of Router, PCs, Server and Switches for VLAN, ACL as well as for STP. Through results and interpretation, it is confirmed that the network is working as intended, with successful failover in STP, proper security via ACLs, and smooth communication between VLANs.

References

(as per the IEEE recommendations)

[1] CompTIA Network+ N10-008 Certification Guide by Glen D. Singh, 2*nd* Edition, Packt publication.

[2] https://www.youtube.com/live/8gCLxDCYJ9Y?si=S4pExAzMRW1wUKDH

[3] https://youtu.be/nmSvoZPNrGQ?si=udFABmYV3uMlDNwc

[4] https://www.geeksforgeeks.org/vlan-acl-vacl/