

Title: Creating VLAN and VLAN Trunking using Packet Tracer

Theory

A VLAN is a logical grouping of devices within a physical network, created to segment network traffic for better performance, security, and management. Devices in the same VLAN can communicate as if they were on the same physical LAN, regardless of their actual location. VLANs are configured on switches using VLAN IDs and help reduce broadcast domains, improve network efficiency, and enhance security by isolating traffic.

VLAN Trunking

VLAN trunking is a technique used to carry traffic from multiple VLANs across a single network link between switches or between a switch and a router. Instead of creating separate physical connections for each VLAN, trunking allows one link to transport multiple VLANs using tags (like IEEE 802.1Q). This helps in efficient use of network resources and enables communication between devices in different VLANs while keeping their traffic logically separated.

VLAN Architecture

VLAN architecture defines how devices are logically segmented within a network to improve performance, security, and management. It consists of:

1. End Devices: Computers, printers, and other network devices assigned to a specific VLAN.
2. Access Layer Switches: Connect end devices and assign them to VLANs via access ports.
3. Trunk Links: Carry traffic from multiple VLANs between switches or to routers.
4. Router or Layer 3 Switch: Enables communication between VLANs (inter-VLAN routing).
5. VLAN IDs: Unique identifiers (1–4094) used to tag frames and distinguish VLAN traffic.

This architecture ensures that devices in the same VLAN communicate as if they are on the same physical network, while isolating traffic between different VLANs.

Component Used

Hardware: Switches (2), Ethernet Cables, End Devices (4)

Software: Cisco Packet Tracer

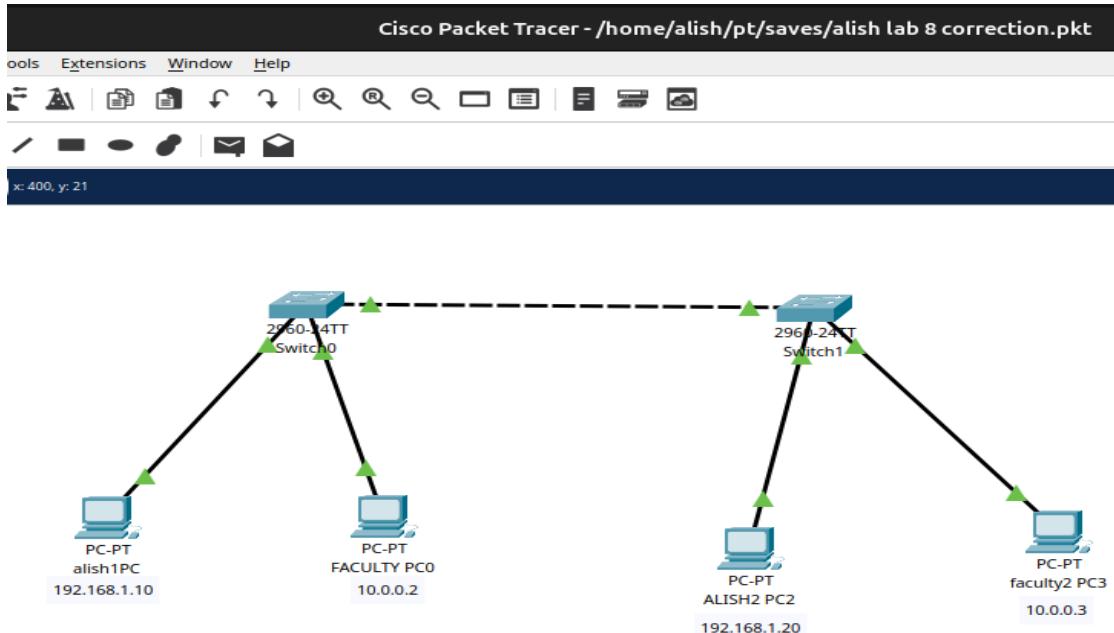


Figure: Network Map for VLAN

Procedure

The procedure for creating the LAN network using Cisco Packet Tracer is shown in the image:

Step 1: Launch Cisco Packet Tracer

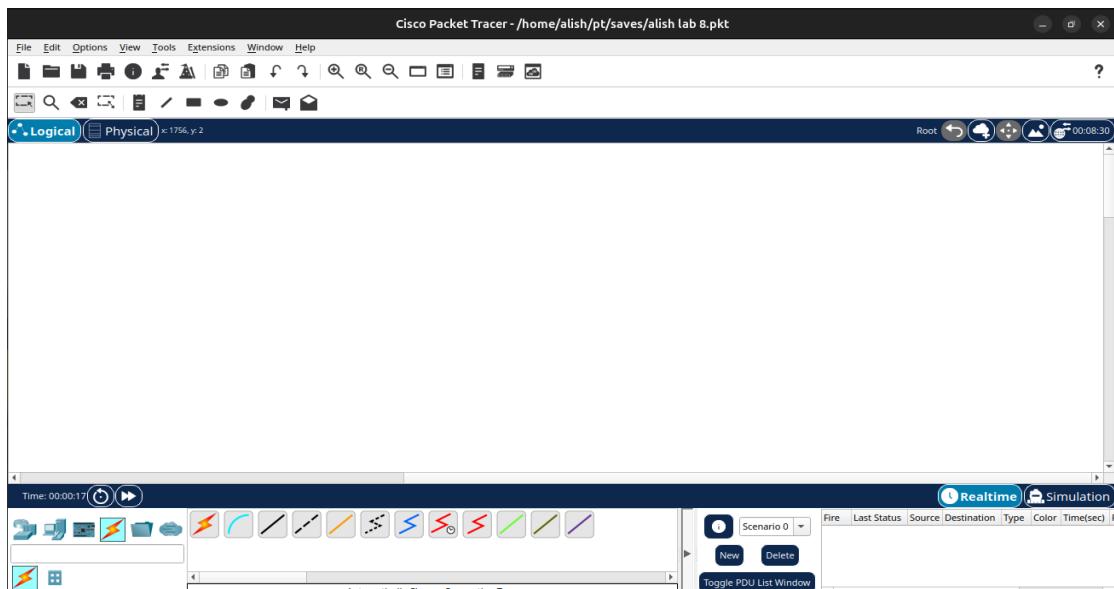


Figure: Workspace for Network Design

Step 2: Add the network devices to the workspace

2.1 From the Device-Type Selection box, choose the following devices and add them to the workspace:

2.2 One 2960-24TT Switch

2.3 Four PCs (labeled PC0, PC1, PC2 and PC3)

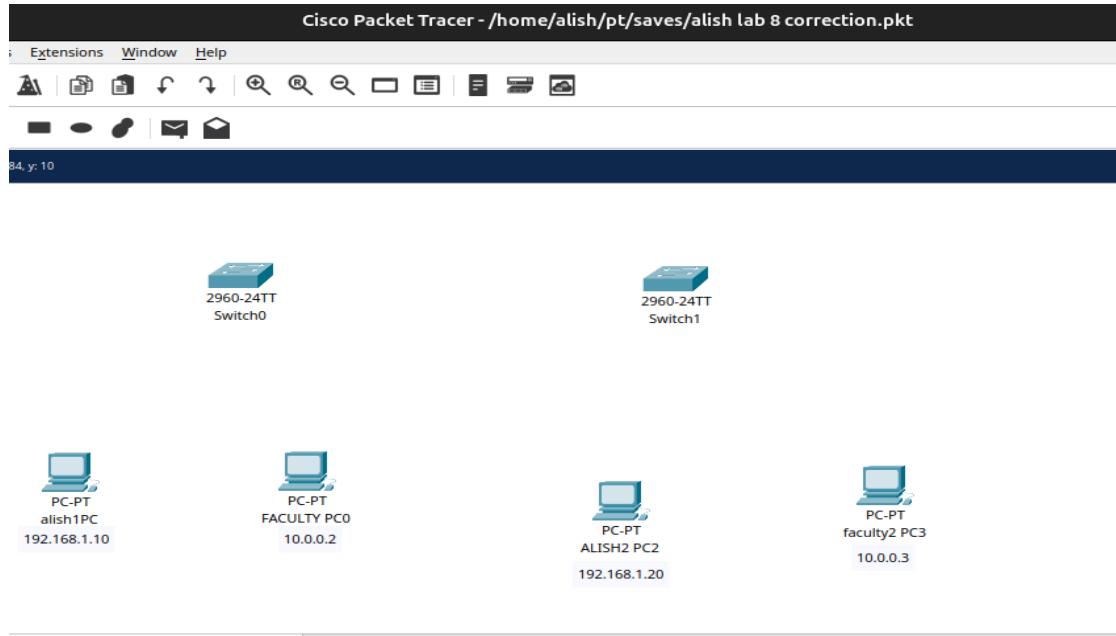


Figure: Switches and PC's for VLAN

Step 3: Connect the devices

3.1 Use the copper straight-through cable to connect each PC to one of the available ports on the switch.

3.2 Ensure that each connection is made properly

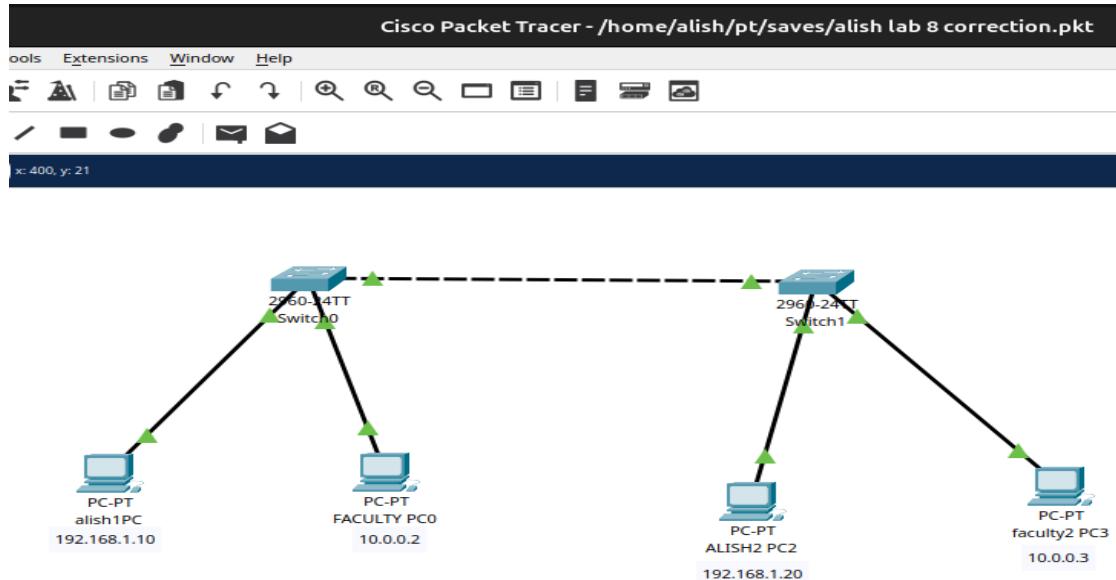


Figure: Connection between Switches and PC's

Step 4: Configure IP address

4.1 Right-click on each PC and select “IP Configuration”.

4.2 In the IP Configuration window, enter the IP address as (192.168.1.10) and 10.0.0.2 for switch0 connected with Alish1 and Faculty1 and for Switch1(192.168.1.20,10.0.0.3) for its Alish2 and Faculty2 , subnet mask and default gateway for each PC.

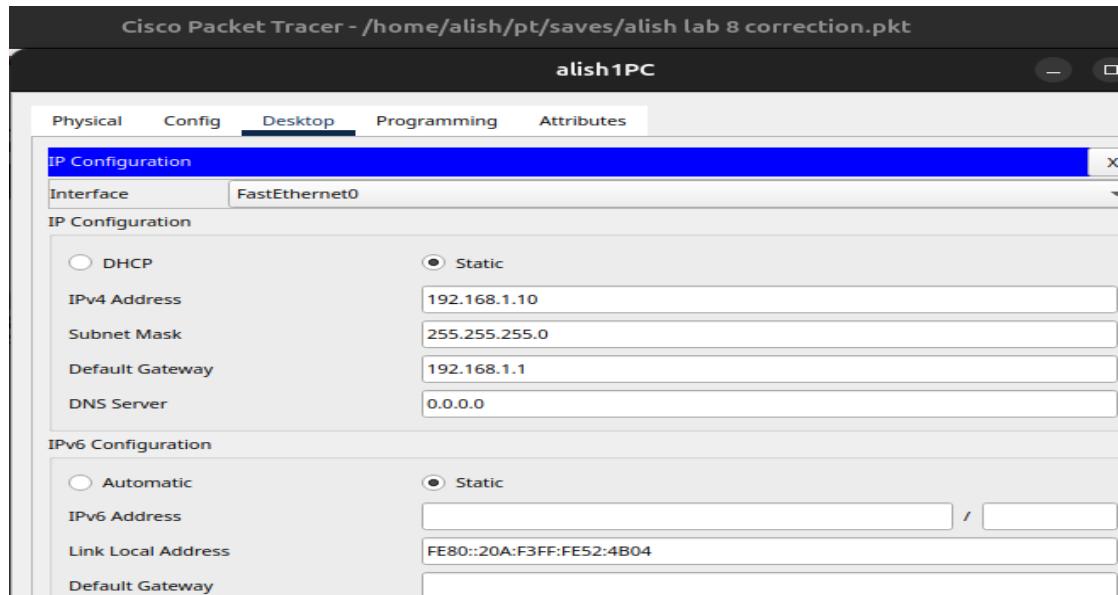


Figure: IP Configuration

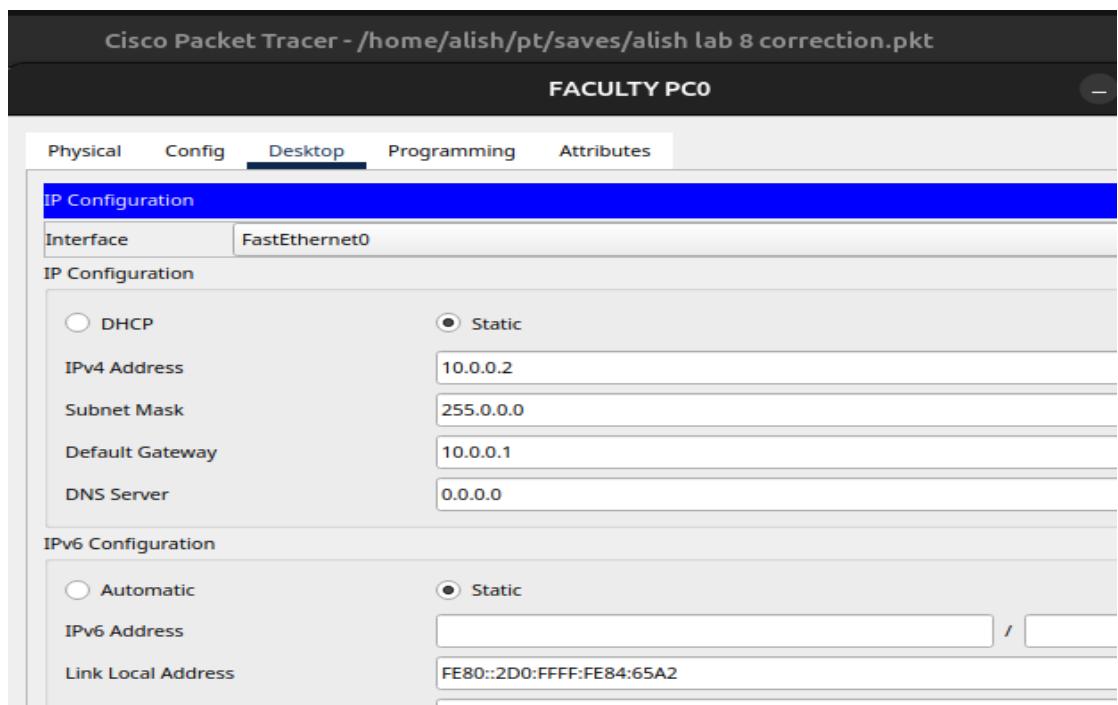


Figure: IP Configuration

Step 5: Configuring VLANs

5.1 Create VLAN on both Switches & assign Port to both switches.

5.2 Create trunkation in the both switches.

Code for VLAN Configurations:

```
Switch>en
Switch#config t
Switch(config)#vlan 10
Switch(config-vlan)#name Alish1
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name Faculty1
Switch(config-vlan)#exit
Switch(config)#exit
```

Code for Assigning ports:

```
Switch#config t
Switch(config) #int fa 0/1
Switch(config-if) #switchport mode access
Switch(config-if) #switchport access vlan 10
Switch(config-if) #int fa 0/2
Switch(config-if) #switchport access vlan 20
Switch(config-if) #exit
Switch(config)#exit
```

The screenshot shows the Cisco Packet Tracer interface with the title bar "Cisco Packet Tracer - /home/alish/pt/saves/lab8 correction.pkt". The main window is titled "Switch0". The terminal window displays the following configuration commands and output:

```
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#show vlan brief
VLAN Name          Status    Ports
----- 
1    default        active    Fa0/3, Fa0/4, Fa0/5, 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   alish1         active    Fa0/1
20   faculty1       active    Fa0/2
1002 fddi-default   active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default   active
Switch#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (10), with
Switch FastEthernet0/1 (1).
```

At the bottom of the terminal window are "Copy" and "Paste" buttons.

Assigning port to VLAN in Switch0

Cisco Packet Tracer - /home/alish/pt/saves/lab8 correction.pkt

Switch1

```

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int fa 0/2
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan brief

VLAN Name          Status      Ports
----  -----
1    default        active     Fa0/3, Fa0/4, Fa0/5, 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   alish2         active     Fa0/1
20   faculty2       active     Fa0/2
1002 fddi-default   active
1003 token-ring-default
1004 fddinet-default
1005 trnet-default   active
Switch#

```

Copy **Paste**

Assigning port on VLAN on Switch 1

Code for Trunking Switches:

```

Switch#config t
Switch(config) #int fa 0/3
Switch(config-if) #switchport mode trunk
Switch(config-if) #exit
Switch(config) #exit

```

Cisco Packet Tracer - /home/alish/pt/saves/lab8 correction.pkt

Switch0

Physical	Config	CLI	Attributes
IOS Command Line Interface			
<pre> 1003 token-ring-default active 1004 fddinet-default active 1005 trnet-default active Switch#config t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#int fa 0/3 Switch(config-if)#switchport mode trunk Switch(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on interface FastEthernet0/3, changed state to down %LINEPROTO-5-UPDOWN: Line protocol on interface FastEthernet0/3, changed state to up Switch(config-if)#exit Switch(config)#exit Switch# %SYS-5-CONFIG_I: Configured from console by console Switch#show vlan brief VLAN Name Status Ports ---- ----- 1 default active Fa0/4, Fa0/5, 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 alish1 active Fa0/1 20 faculty1 active Fa0/2 1002 fddi-default active 1003 token-ring-default 1004 fddinet-default 1005 trnet-default active Switch# </pre>			

Figure:Configuring trunking between switches

-Alish Thapa

Cisco Packet Tracer - /home/alish/pt/saves/lab8 correction.pkt

Switch1

```

Switch#int f 0/3
^
% Invalid input detected at '^' marker.

Switch#show vlan brief

VLAN Name          Status    Ports
-----  -----
1     default       active    Fa0/4, Fa0/5, 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    alish2        active    Fa0/1
20    faculty2      active    Fa0/2
1002   fddi-default active
1003   token-ring-default active
1004   fddinet-default active
1005   trnet-default   active
Switch#

```

Copy P

Figure: Configuring trunking between switches

6: Testing and Validation

- 6.1 Use the ping command from each PC to check network connectivity.
- 6.2 Open Command Prompt and type *ping <IP address of another PC>*.
- 6.3 If replies are received, the connection is successful.

Cisco Packet Tracer - /home/alish/pt/saves/lab8 correction.pkt

faculty2 pc3

```

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.2:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

```

Figure: Connectivity test between network Faculty2 10.0.0.2 and Faculty1 10.0.0.1

2 DEC 10:51

Cisco Packet Tracer - /home/alish/pt/saves/lab8 correction.pkt

alish1PC

```
C:\>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:

Reply from 192.168.1.20: bytes=32 time=52ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 52ms, Average = 13ms

C:\>
```

Figure: Connectivity test between network Alish1 192.168.1.10 and Alish2

192.168.1.12

6.4 We can't ping Alish1 and Faculty1 as VLAN10 (Alish) and VLAN 20 (Faculty1)
As are in separate VLANS

Cisco Packet Tracer - /home/alish/pt/saves/lab8 correction.pkt

alish1PC

```
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figure:Connectivity failure between Alish1(192.168.10) and Faculty1
(10.0.0.2)

Addressing Table:

Device	Interface	IPv4 Address	Subnet mask	Switch port	VLAN	VLAN NO.	Link
Alish1	NIC	192.168.1.10	255.255.255.0	Switch fa0/1	10	Alish1	Access
Alish2	NIC	192.168.1.20	255.255.255.0	Switch fa0/1	10	Alish2	Access
Faculty 1	NIC	10.0.0.2	255.0.0.0	Switch fa0/2	20	Faculty 1	Access
Faculty 2	NIC	10.0.0.3	255.0.0.0	Switch fa0/2	20	Faculty 2	Access

Conclusion

In this lab, VLANs were successfully configured to logically segment a network using Cisco Packet Tracer. Access ports were assigned to specific VLANs, and trunk links were set up to allow multiple VLANs to communicate across switches. The lab demonstrated how VLANs improve network management, enhance security, and reduce broadcast traffic. Overall, the experiment reinforced the understanding of VLAN architecture, trunking, and inter-VLAN communication.