Lab 2: VLAN, Inter-VLAN Routing and EtherChannel Redundancy with Troubleshooting & Hardening

Table of contents

1. Lab Metadata

- **Lab Name:** VLAN Inter-VLAN Routing and EtherChannel Redundancy with Troubleshooting & Hardening .
- **Tools:** Cisco Packet Tracer.
- **Devices:** 3x Cisco Catalyst Switches (CORE and ACCESS), Cisco Router (R1), End Devices (PCs).
- **Scope:** Layer 2 and Layer 3 network configuration, redundancy testing, troubleshooting, and basic security hardening.

2. Overview

This lab focuses on building and verifying a multi-VLAN network with inter-VLAN routing using a router-on-a-stick (ROAS) design. In addition to basic VLAN and DHCP configuration, the lab introduces EtherChannel for link redundancy between switches.

The lab also includes troubleshooting scenarios and verification checkpoints to document the network state before and after corrections. Final steps focus on basic device hardening and secure management access using SSH.

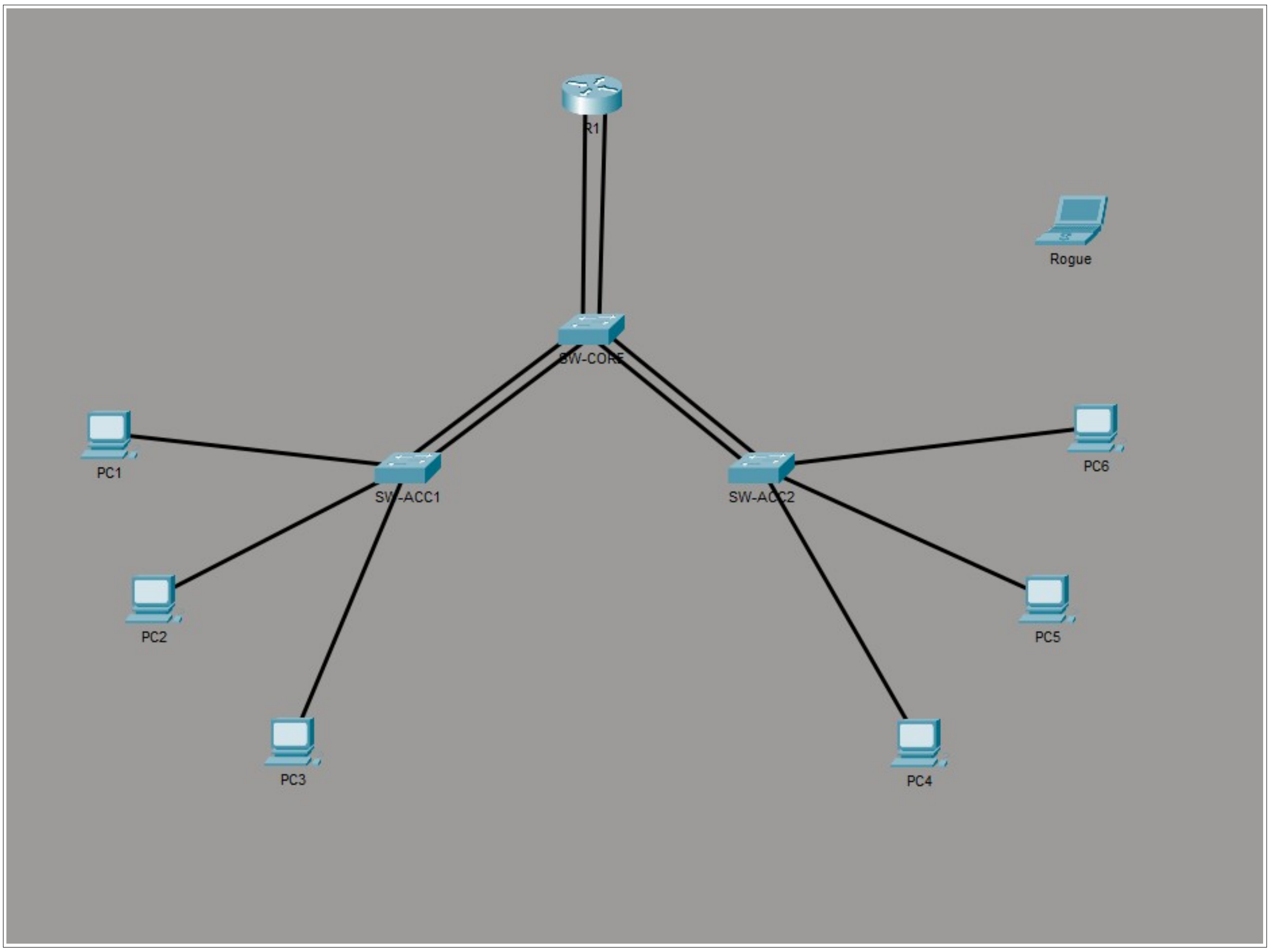
2.1. Objectives

- Configure VLANs and assign access ports.
- Configure trunk links between switches and router.
- Implement inter-VLAN routing using ROAS
- Configure DHCP for end devices
- Configure EtherChannel for link redundancy
- Verify Layer 2 and Layer 3 operation
- Perform failure testing and document redundancy behavior
- Apply basic device hardening and secure management access

3. Network Topology

The LAB2 network topology is designed to simulate a small enterprise environment with multiple VLANs, centralized switching, and redundant uplinks between switches. The topology includes one router performing inter-VLAN routing and multiple switches operating at the access and core layers.

The network is segmented into multiple VLANs to seprate user traffic and management traffic. Inter-VLAN communication is achieved using router-on-a-stick (ROAS) configuration on the router.



SCREEN #1 - Network topology

3.1. Topology Summary

The topology consists of the following components:

- One router (R1) providing inter-VLAN routing and DHCP services
- One core switch (SW-CORE) responsible for VLAN trunking and EtherChannel aggregation
- Access switches (SW-ACC1, SW-ACC2) connecting end devices
- Multiple VLANs for user networks and management access
- Redundant links between core and access switches implemented using EtherChannel

The design ensures logical separation of traffic, centralized routing, and increased link availability through EtherChannel redundancy.

4. IP Addressing Plan

Before starting the configuration, an IP addressing plan was prepared to clearly define how VLANs are separated and how routing between them would work. Each VLAN uses its own subnet, which makes the network easier to manage, troubleshoot, and expand.

The addressing scheme is intentionally simple and predictable. This helps during verification and troubleshooting, especially when working with inter-VLAN routing and DHCP.

4.1. VLANs and Subnet Allocation

The network is divided into multiple VLANs, each with a clearly defined role. VLAN names are used to improve readability and make the configuration easier to understand and maintain:

- VLAN 10 – USERS

  Subnet: 192.168.10.0/24

  Used for standard user endpoints.

- VLAN 20 – OFFICE

  Subnet: 192.168.20.0/24

  Used for office-related devices.

- VLAN 30 – GUEST

  Subnet: 192.168.30.0/24

  Used for guest endpoints, logically separated from internal networks.

- VLAN 99 – MGMT

  Subnet: 192.168.99.0/24

  Dedicated management VLAN used for administrative access to network devices

- VLAN 999 – PARKING

  No IP subnet assigned.

  Used as a parking VLAN for unused switch ports.

Each routed VLAN is associated with a router-on-a-stick subinterface on R1, which provides the default gateway. IP addresses for end devices are assigned dynamically via DHCP, while the management VLAN is reserved for device access and administration.

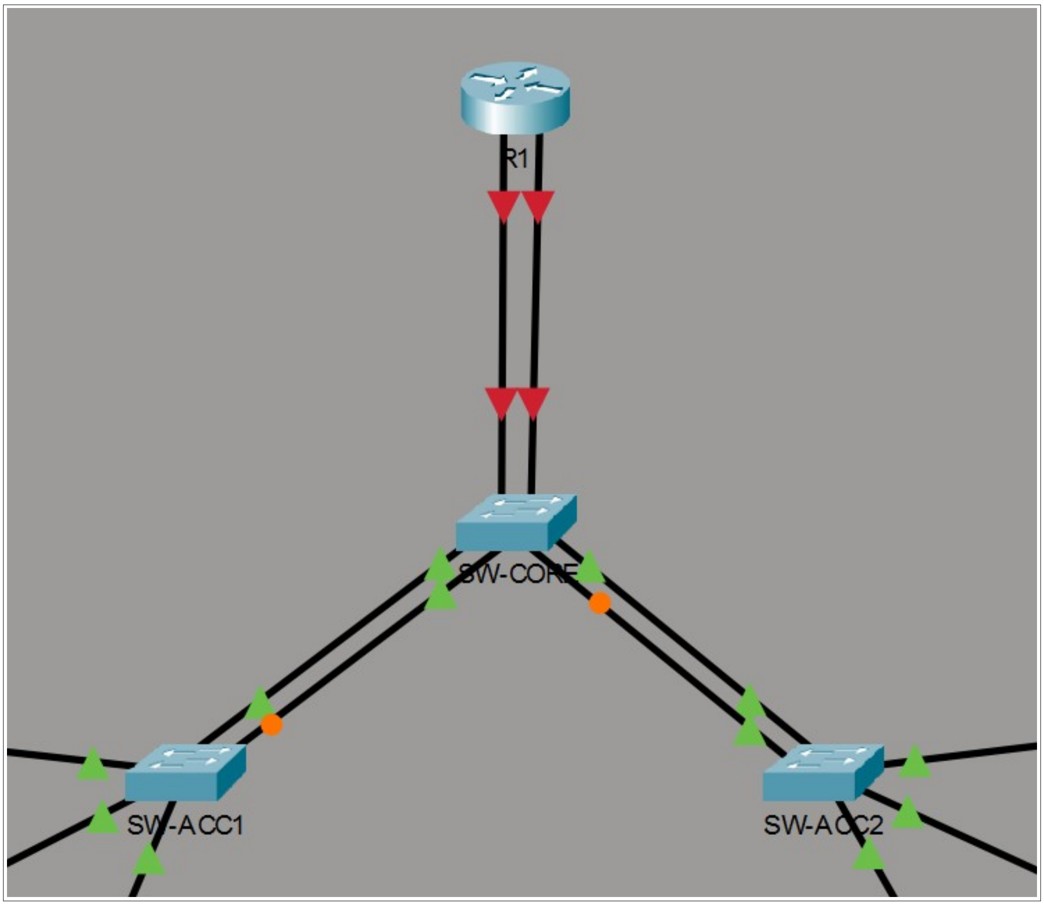
5. Step-by-Step Implementation

This section describes the configuration process step by step, starting from building the topology and basic device preparation, through VLAN and trunk configuration, and ending with routing and redundancy features. All configuration steps are verified using dedicated screenshots.

5.1. Build the Topology (Packet Tracer)

The first step was to build the logical topology in Cisco Packet Tracer according to the planned design. Devices were placed and interconnected to reflect a simple core–access architecture with redundant uplinks between switches.

At this stage, the focus was only on correct device placement and cabling, without any configuration applied yet. The topology used in this lab is shown in Section 3 (Network Topology).

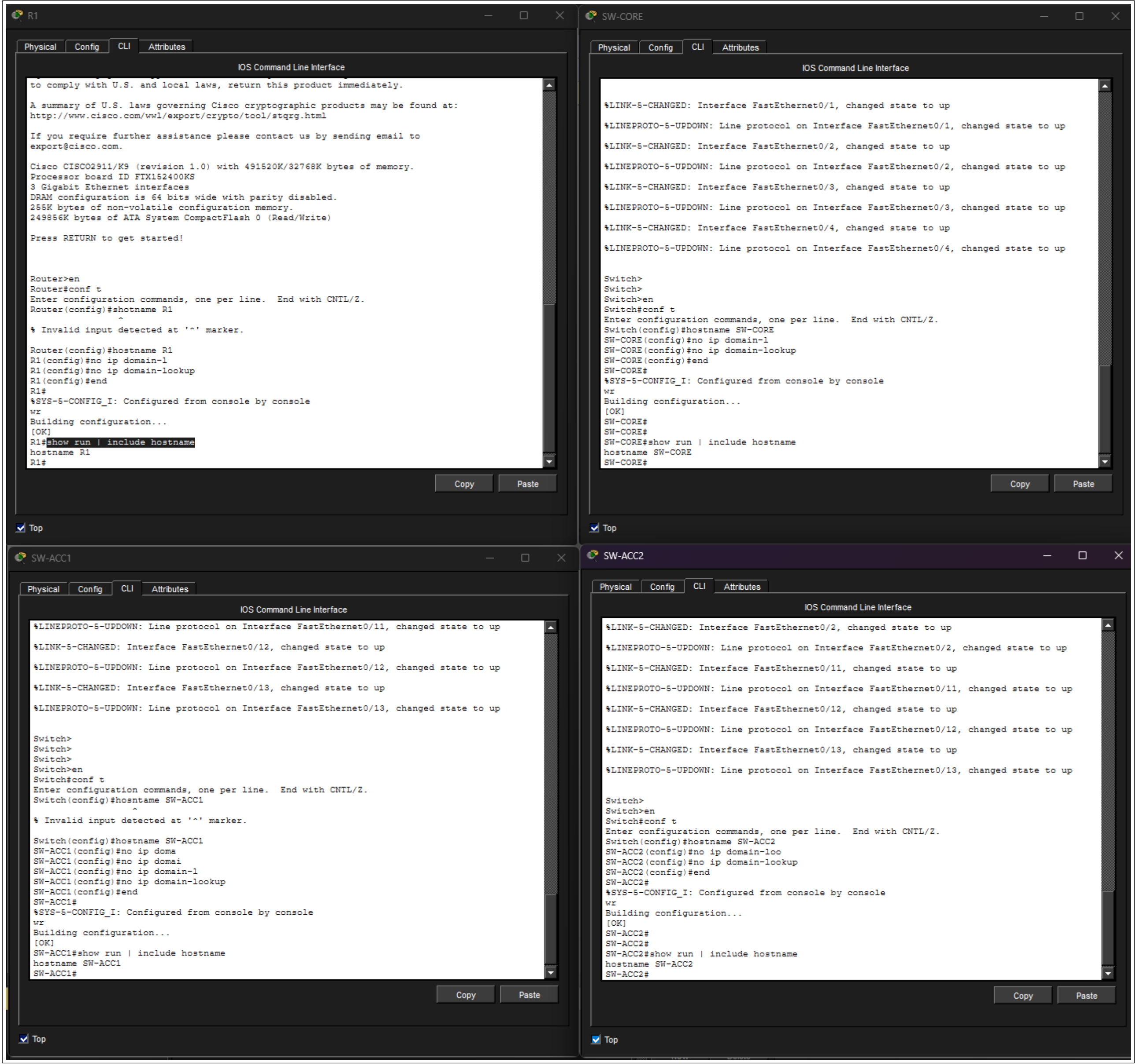


SCREEN #2 - Physical cabling

5.2. Device Basic Setup

Basic configuration was applied to all network devices to prepare them for further configuration. This included setting hostnames and disabling unnecessary defaults.

Hostnames were configured to clearly identify device roles within the topology (CORE, ACCESS, Router).



```
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO2911/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
3 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!



Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#shotname R1
                ^
% Invalid input detected at '^' marker.

Router(config)#hostname R1
R1(config)#no ip domain-l
R1(config)#no ip domain-lookup
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
R1#show run | include hostname
hostname R1
R1#
```

```

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

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

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

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

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


Switch>
Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-CORE
SW-CORE(config)#no ip domain-l
SW-CORE(config)#no ip domain-lookup
SW-CORE(config)#end
SW-CORE#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
SW-CORE#
SW-CORE#
SW-CORE#show run | include hostname
hostname SW-CORE
SW-CORE#
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/12, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/13, changed state to up


Switch>
Switch>
Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hosntame SW-ACC1
                  ^
% Invalid input detected at '^' marker.

Switch(config)#hostname SW-ACC1
SW-ACC1(config)#no ip doma
SW-ACC1(config)#no ip domai
SW-ACC1(config)#no ip domain-l
SW-ACC1(config)#no ip domain-lookup
SW-ACC1(config)#end
SW-ACC1#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
SW-ACC1#show run | include hostname
hostname SW-ACC1
SW-ACC1#
```

```
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/12, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/13, changed state to up


Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-ACC2
SW-ACC2(config)#no ip domain-loo
SW-ACC2(config)#no ip domain-lookup
SW-ACC2(config)#end
SW-ACC2#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
SW-ACC2#
SW-ACC2#
SW-ACC2#show run | include hostname
hostname SW-ACC2
SW-ACC2#
```

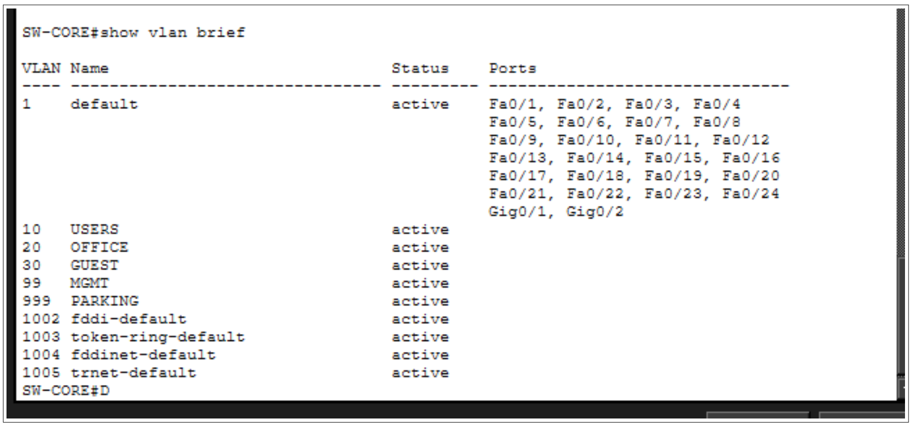
SCREEN #3 - Hostname configuration

5.3. VLAN Creation

VLANs were created on the switches according to the addressing plan. Each VLAN was assigned a descriptive name to improve readability and simplify troubleshooting.

Configured VLANs:

- VLAN 10 - USERS
- VLAN 20 - OFFICE
- VLAN 30 - GUEST
- VLAN 99 - MGMT
- VLAN 999 - PARKING



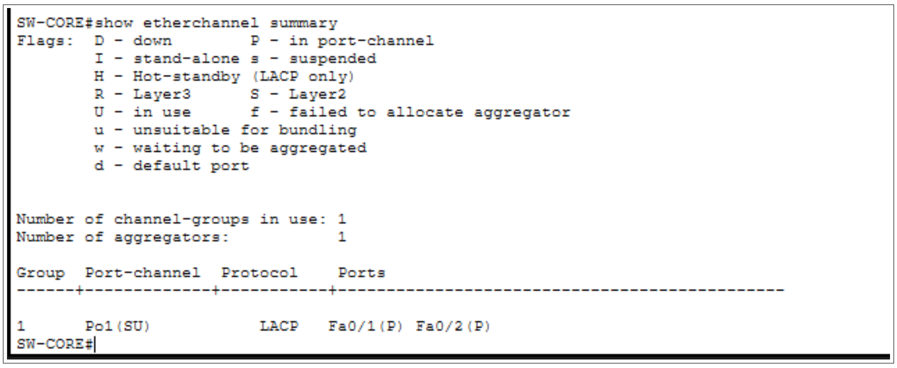
```
SW-CORE#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, 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   USERS                            active    
20   OFFICE                           active    
30   GUEST                            active    
99   MGMT                             active    
999  PARKING                          active    
1002 fddi-default                     active    
1003 token-ring-default               active    
1004 fddinet-default                  active    
1005 trnet-default                    active    
SW-CORE#D
```

SCREEN #4 - show vlan brief (SW-CORE)

5.4. EtherChannel Configuration (CORE–ACCESS)

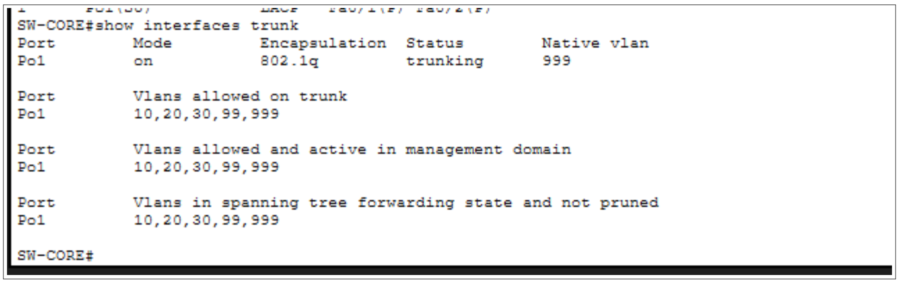
To increase bandwidth and provide link redundancy between the core and access layer, EtherChannel was configured between SW-CORE and the access switches. Multiple physical links were bundled into logical port-channels using LACP, allowing the network to continue operating even if one link fails.

After configuration, EtherChannel status and trunk operation were verified on both the core and access switches to confirm that all member interfaces were correctly aggregated and forwarding traffic.



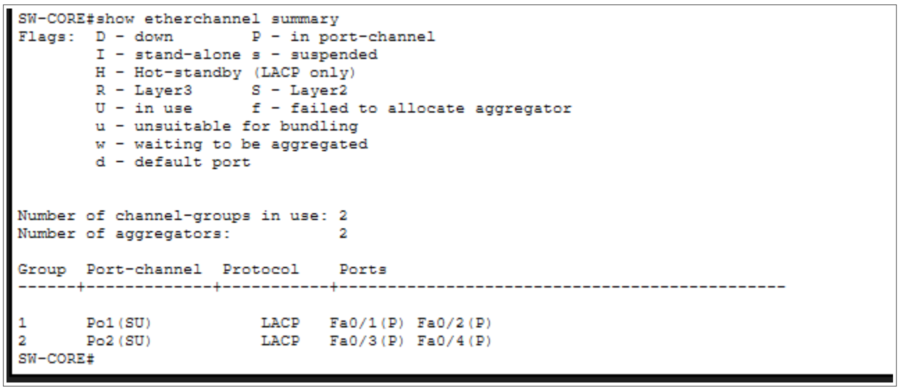
```
SW-CORE#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting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


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

Group  Port-channel  Protocol    Ports
------+-------------+-----------+----------------------------------------------

1      Po1(SU)           LACP   Fa0/1(P)  Fa0/2(P)
SW-CORE#
```

SCREEN #5 - show etherchannel summary (SW-CORE)



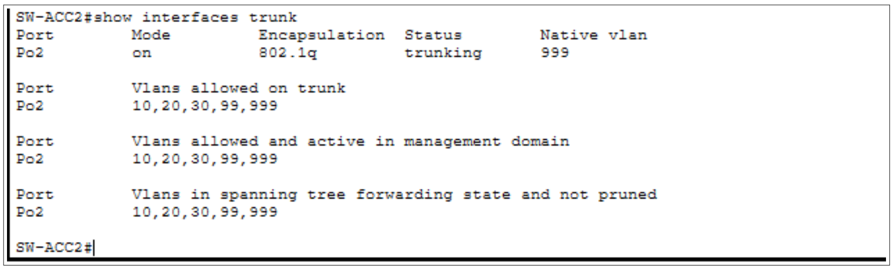
```
1      Po1(SU)           LACP   Fa0/1(P)  Fa0/2(P)
SW-CORE#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      999

Port        Vlans allowed on trunk
Po1         10,20,30,99,999

Port        Vlans allowed and active in management domain
Po1         10,20,30,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Po1         10,20,30,99,999

SW-CORE#
```

SCREEN #6 - show interfaces trunk (SW-CORE)



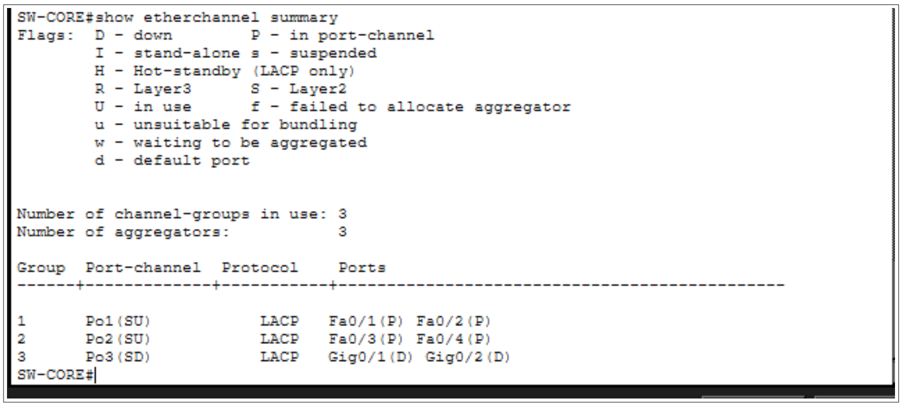
```
SW-CORE#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting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


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+----------------------------------------------

1      Po1(SU)           LACP   Fa0/1(P)  Fa0/2(P)
2      Po2(SU)           LACP   Fa0/3(P)  Fa0/4(P)
SW-CORE#
```

SCREEN #7 - show etherchannel summary (SW-CORE)



```
SW-ACC2#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Po2         on           802.1q         trunking      999

Port        Vlans allowed on trunk
Po2         10,20,30,99,999

Port        Vlans allowed and active in management domain
Po2         10,20,30,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Po2         10,20,30,99,999

SW-ACC2#
```

SCREEN #8 - show interfaces trunk (SW-ACC2)



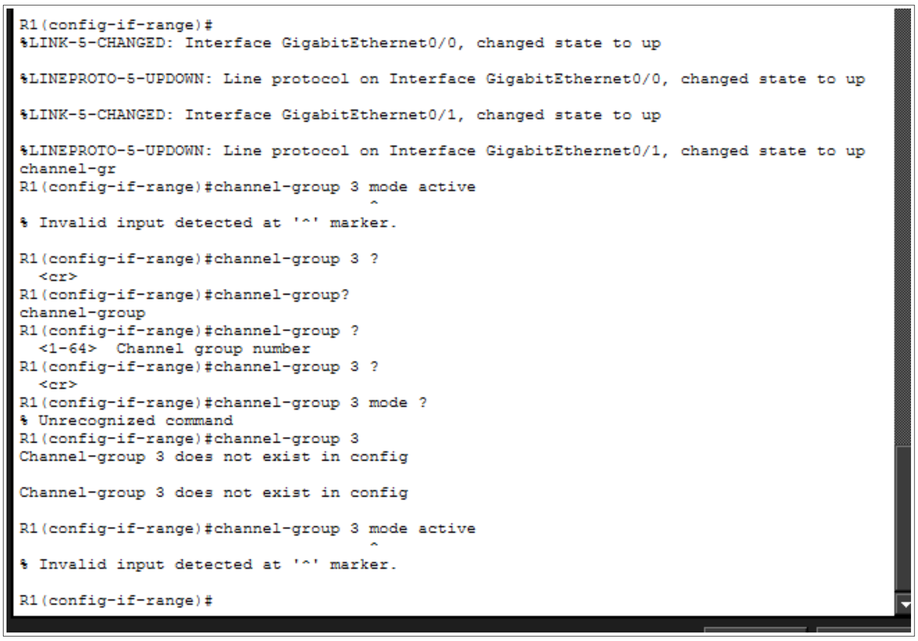
```
SW-CORE#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting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


Number of channel-groups in use: 3
Number of aggregators:           3

Group  Port-channel  Protocol    Ports
------+-------------+-----------+----------------------------------------------

1      Po1(SU)           LACP   Fa0/1(P) Fa0/2(P)
2      Po2(SU)           LACP   Fa0/3(P) Fa0/4(P)
3      Po3(SD)           LACP   Gig0/1(D) Gig0/2(D)
SW-CORE#
```

SCREEN #9 — show etherchannel summary (SW-CORE)

5.5. Packet Tracer Limitation - EtherChannel on Router

During the implementation of EtherChannel, an attempt was made to configure a port-channel on the router interface. This resulted in an error, as Cisco Packet Tracer does not support EtherChannel configuration on router platforms.

This behavior was identified as a tool limitation, not a configuration mistake. As a result, the design was adjusted to use a single physical trunk link between the router and the core switch, while EtherChannel remained in use only between the core and access switches.



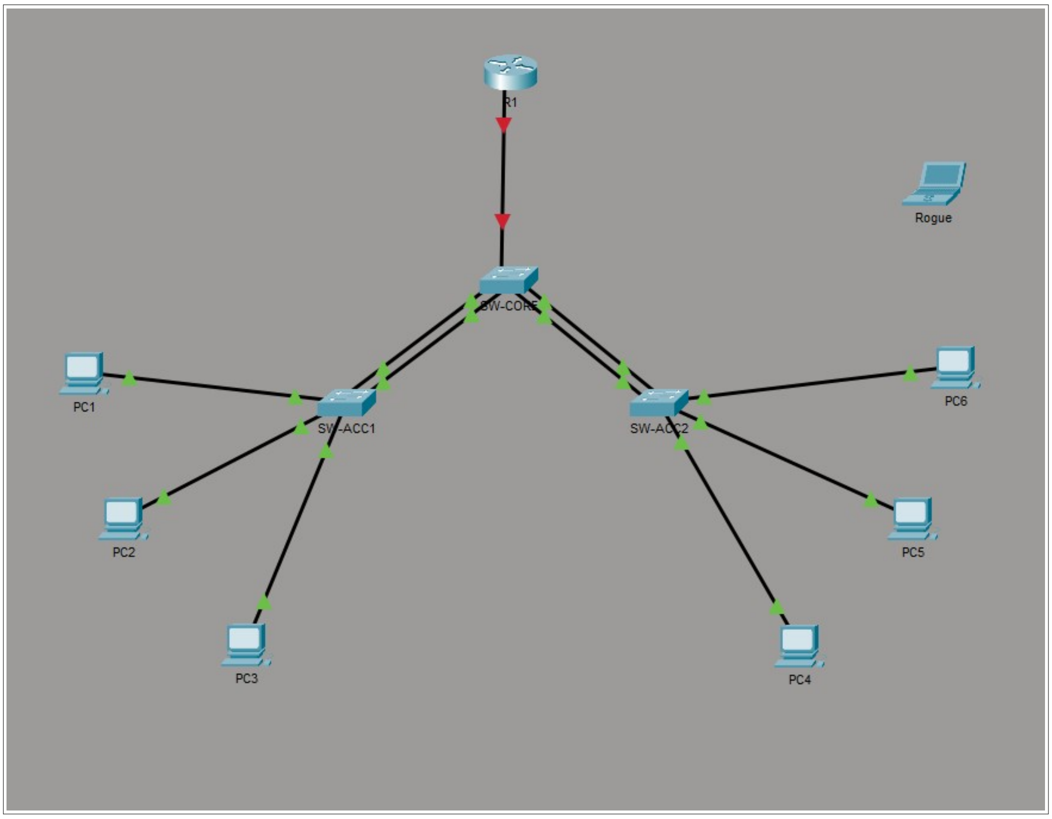
```
R1(config-if-range)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

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

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
channel-gr
R1(config-if-range)#channel-group 3 mode active
                                    ^
% Invalid input detected at '^' marker.

R1(config-if-range)#channel-group 3 ?
  <cr>
R1(config-if-range)#channel-group?
channel-group
R1(config-if-range)#channel-group ?
  <1-64>  Channel group number
R1(config-if-range)#channel-group 3 ?
  <cr>
R1(config-if-range)#channel-group 3 mode ?
% Unrecognized command
R1(config-if-range)#channel-group 3
Channel-group 3 does not exist in config

Channel-group 3 does not exist in config

R1(config-if-range)#channel-group 3 mode active
                                    ^
% Invalid input detected at '^' marker.

R1(config-if-range)#
```

SCREEN #10—– Error no EtherChannel support on 2911 router - Packet Tracer limitation

5.6. Topology Correction After Packet Tracer Limitation

After identifying the Packet Tracer limitation related to EtherChannel on the router, the network topology was adjusted accordingly. The router was connected to the core switch using a single trunk link, while EtherChannel connections were preserved only between the core and access switches.

This correction ensured full compatibility with the simulation environment while maintaining redundancy and proper Layer 2 operation within the campus network.

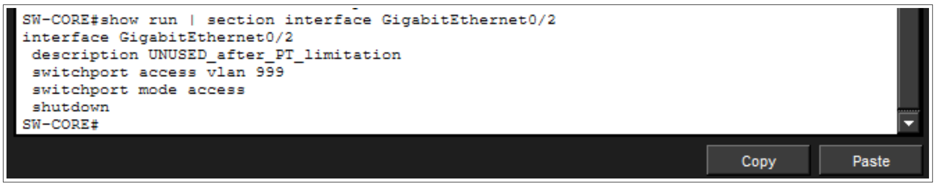


SCREEN #11 - Corrected network topology

5.7. Inter-VLAN Routing (ROAS) Configuration and Correction

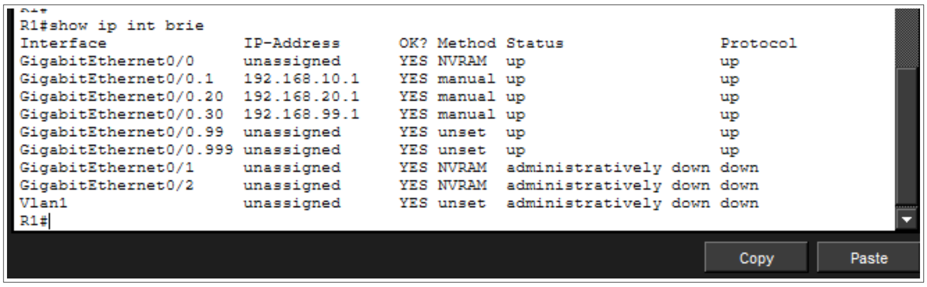
Inter-VLAN routing was implemented on **Router R1** using the **router-on-a-stick (ROAS)** approach. Subinterfaces were created on the router's physical interface and associated with the corresponding VLANs using IEEE 802.1Q encapsulation.

During verification, an initial misconfiguration of one subinterface was identified. The issue was corrected by adjusting the subinterface numbering to properly match the VLAN ID, after which interface status and IP addressing were revalidated.



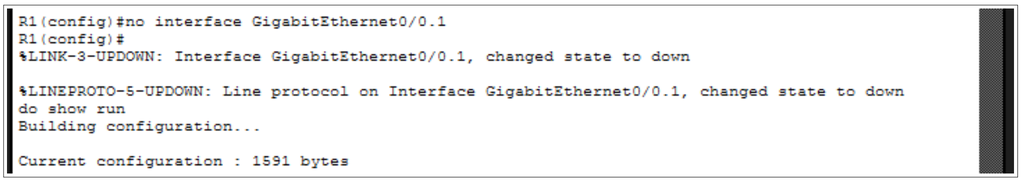
```
SW-CORE#show run | section interface GigabitEthernet0/2
interface GigabitEthernet0/2
 description UNUSED_after_PT_limitation
 switchport access vlan 999
 switchport mode access
 shutdown
SW-CORE#
```

SCREEN #12 - show running-config (router subinterfaces)



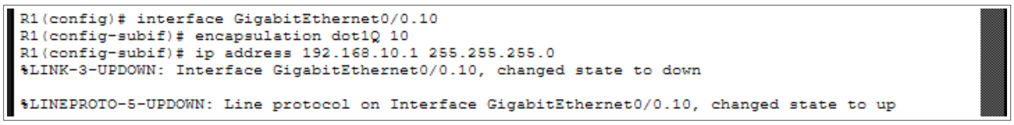
```
R1#show ip int brie
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES NVRAM  up                    up
GigabitEthernet0/0.1   192.168.10.1    YES manual up                    up
GigabitEthernet0/0.20  192.168.20.1    YES manual up                    up
GigabitEthernet0/0.30  192.168.99.1    YES manual up                    up
GigabitEthernet0/0.99  unassigned      YES unset  up                    up
GigabitEthernet0/0.999 unassigned      YES unset  up                    up
GigabitEthernet0/1     unassigned      YES NVRAM  administratively down down
GigabitEthernet0/2     unassigned      YES NVRAM  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
R1#
```

SCREEN #13 - show ip interface brief (initial verification)



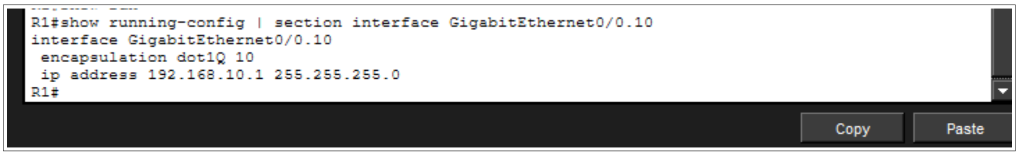
```
R1(config)#no interface GigabitEthernet0/0.1
R1(config)#
%LINK-3-UPDOWN: Interface GigabitEthernet0/0.1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.1, changed state to down
do show run
Building configuration...

Current configuration : 1591 bytes
```

SCREEN #29 - ROAS subinterface correction (Gi0.1 to Gi0.10)



```
R1(config)# interface GigabitEthernet0/0.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
%LINK-3-UPDOWN: Interface GigabitEthernet0/0.10, changed state to down

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

SCREEN #30 — ROAS correction verification



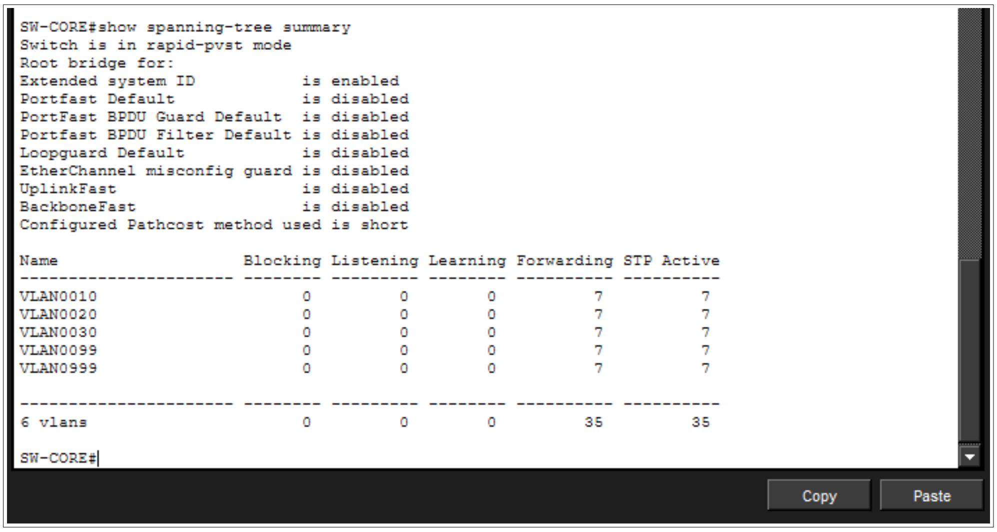
```
R1#show running-config | section interface GigabitEthernet0/0.10
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
R1#
```

SCREEN #31 - ROAS correction verification

5.8. Spanning Tree Verification (CORE as Root Bridge)

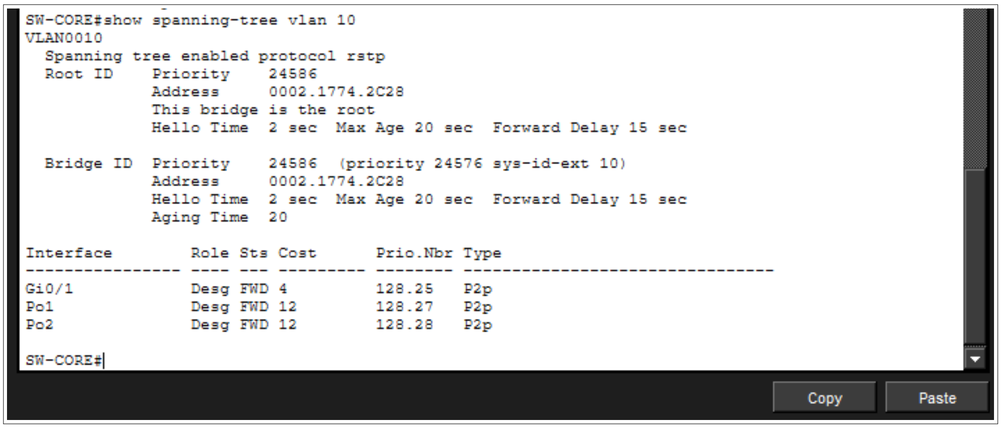
Spanning Tree Protocol (STP) was verified to ensure a stable Layer 2 topology and to confirm that the core switch (SW-CORE) is operating as the root bridge for the user VLANs.

STP status was checked globally and per VLAN to validate correct root bridge election and port roles. This step ensures predictable traffic flow and proper interaction with EtherChannel links.



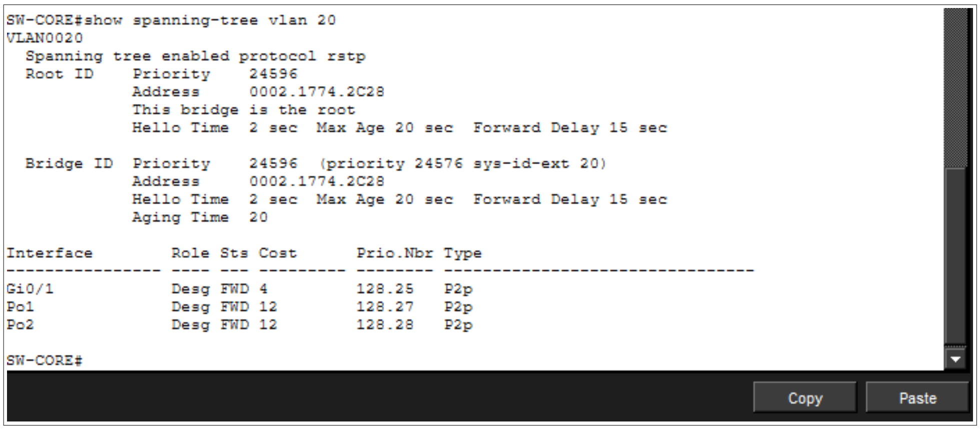
```
SW-CORE#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for:
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0010                     0         0        0          7          7
VLAN0020                     0         0        0          7          7
VLAN0030                     0         0        0          7          7
VLAN0099                     0         0        0          7          7
VLAN0999                     0         0        0          7          7

---------------------- -------- --------- -------- ---------- ----------
6 vlans                      0         0        0         35         35

SW-CORE#
```

SCREEN #14 - show spanning-tree summary (SW-CORE)



```
SW-CORE#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    24586
             Address     0002.1774.2C28
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24586  (priority 24576 sys-id-ext 10)
             Address     0002.1774.2C28
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Desg FWD 4         128.25   P2p
Po1              Desg FWD 12        128.27   P2p
Po2              Desg FWD 12        128.28   P2p

SW-CORE#
```

SCREEN #15 - show spanning-tree vlan 10



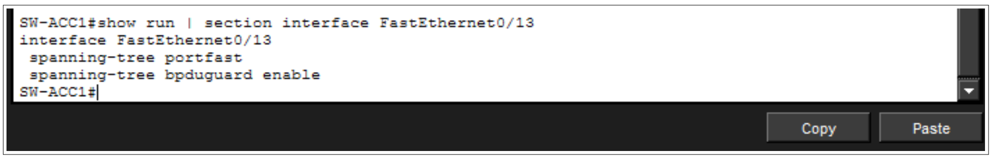
```
SW-CORE#show spanning-tree vlan 20
VLAN0020
  Spanning tree enabled protocol rstp
  Root ID    Priority    24596
             Address     0002.1774.2C28
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24596  (priority 24576 sys-id-ext 20)
             Address     0002.1774.2C28
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Desg FWD 4         128.25   P2p
Po1              Desg FWD 12        128.27   P2p
Po2              Desg FWD 12        128.28   P2p

SW-CORE#
```

SCREEN #16 - show spanning-tree vlan 20

5.9. Access Ports Configuration & Parking VLAN

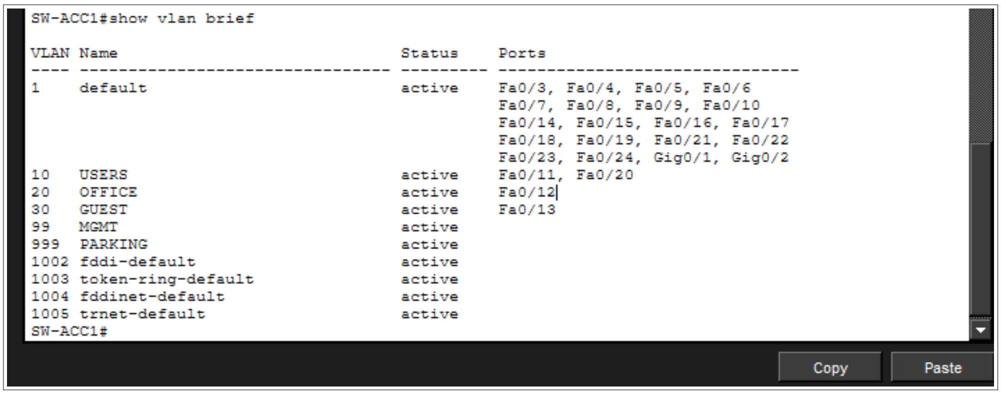
Access ports on the access switches were configured and assigned to the appropriate VLANs (USERS, OFFICE, GUEST). This ensures that end devices are placed directly into the correct network segment without relying on trunking.

Unused switch ports were moved to VLAN 999 (PARKING) as a basic security measure to prevent unintended access. Port configuration and VLAN membership were verified on the access switch.



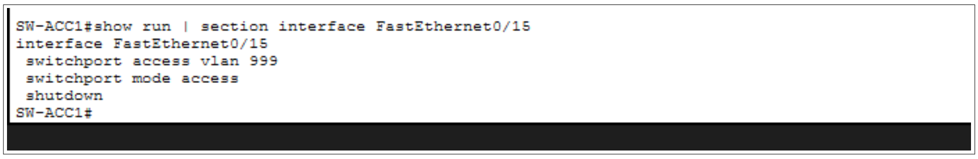
```
SW-ACC1#show run | section interface FastEthernet0/13
interface FastEthernet0/13
 spanning-tree portfast
 spanning-tree bpduguard enable
SW-ACC1#
```

SCREEN #17 - show running-config interface Fa0/11 (access port configuration)



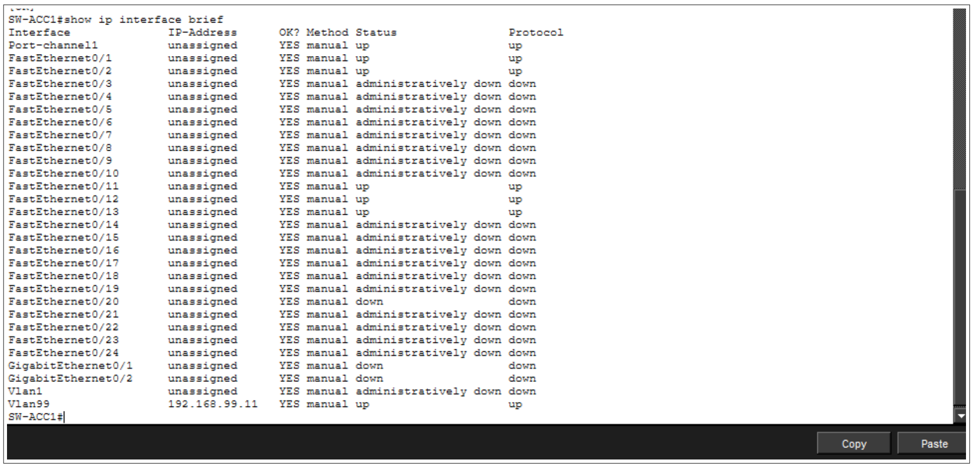
```
SW-ACC1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   USERS                            active    Fa0/11, Fa0/20
20   OFFICE                           active    Fa0/12
30   GUEST                            active    Fa0/13
99   MGMT                             active
999  PARKING                          active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SW-ACC1#
```

SCREEN #18 - show vlan brief (SW-ACC1)



```
SW-ACC1#show run | section interface FastEthernet0/15
interface FastEthernet0/15
 switchport access vlan 999
 switchport mode access
 shutdown
SW-ACC1#
```

SCREEN #19 — show running-config interface Fa0/15 (PARKING VLAN)



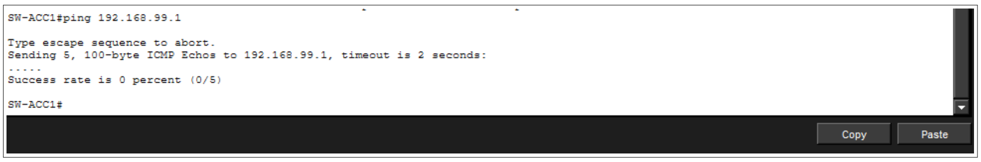
```
SW-ACC1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Port-channel1          unassigned      YES manual up                    up
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual administratively down down
FastEthernet0/4        unassigned      YES manual administratively down down
FastEthernet0/5        unassigned      YES manual administratively down down
FastEthernet0/6        unassigned      YES manual administratively down down
FastEthernet0/7        unassigned      YES manual administratively down down
FastEthernet0/8        unassigned      YES manual administratively down down
FastEthernet0/9        unassigned      YES manual administratively down down
FastEthernet0/10       unassigned      YES manual administratively down down
FastEthernet0/11       unassigned      YES manual up                    up
FastEthernet0/12       unassigned      YES manual up                    up
FastEthernet0/13       unassigned      YES manual up                    up
FastEthernet0/14       unassigned      YES manual administratively down down
FastEthernet0/15       unassigned      YES manual administratively down down
FastEthernet0/16       unassigned      YES manual administratively down down
FastEthernet0/17       unassigned      YES manual administratively down down
FastEthernet0/18       unassigned      YES manual administratively down down
FastEthernet0/19       unassigned      YES manual administratively down down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual administratively down down
FastEthernet0/22       unassigned      YES manual administratively down down
FastEthernet0/23       unassigned      YES manual administratively down down
FastEthernet0/24       unassigned      YES manual administratively down down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  unassigned      YES manual administratively down down
Vlan99                 192.168.99.11   YES manual up                    up
SW-ACC1#
```

SCREEN #20 - show ip interface brief (SW-ACC1)

5.10. Management VLAN (VLAN 99) Connectivity Issue

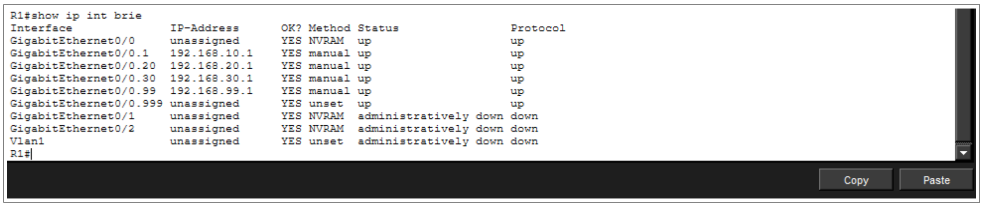
During verification, connectivity to the management VLAN (VLAN 99) was tested from the access switch. The initial ping to the default gateway (192.168.99.1) failed, indicating an addressing or configuration issue.

After reviewing the router configuration, the IP addressing was corrected. Once the change was applied, connectivity to the management VLAN was successfully restored.



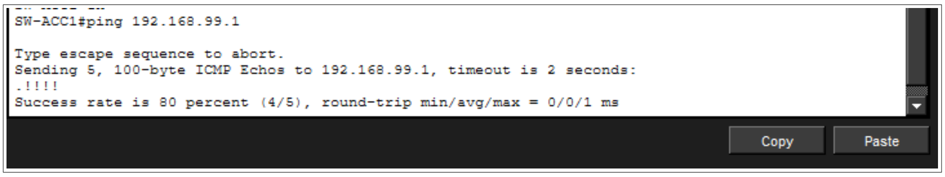
```
SW-ACC1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-ACC1#
```

SCREEN #21 - ping failed (SW-ACC1 to 192.168.99.1)



```
R1#show ip int brie
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES NVRAM  up                    up
GigabitEthernet0/0.1   192.168.10.1    YES manual up                    up
GigabitEthernet0/0.20  192.168.20.1    YES manual up                    up
GigabitEthernet0/0.30  192.168.30.1    YES manual up                    up
GigabitEthernet0/0.99  192.168.99.1    YES manual up                    up
GigabitEthernet0/0.999 unassigned      YES unset  up                    up
GigabitEthernet0/1     unassigned      YES NVRAM  administratively down down
GigabitEthernet0/2     unassigned      YES NVRAM  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
R1#
```

SCREEN #22 - IP addressing correction (R1)



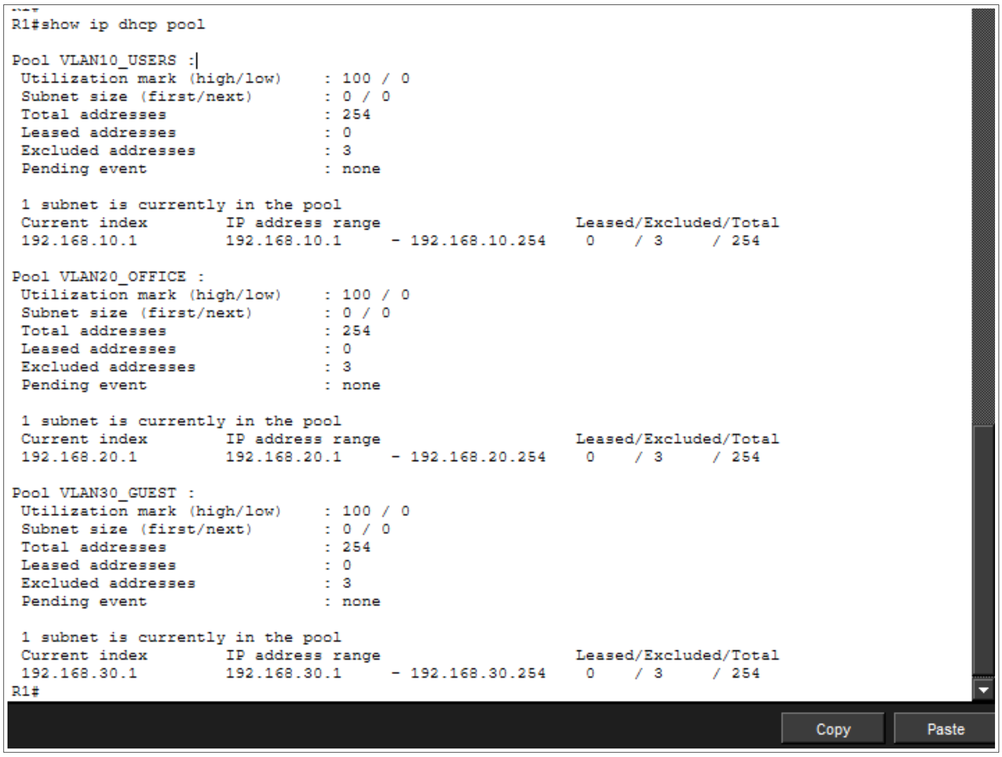
```
SW-ACC1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
```

SCREEN #23 - ping successful (SW-ACC1)

5.11. DHCP Configuration and Troubleshooting

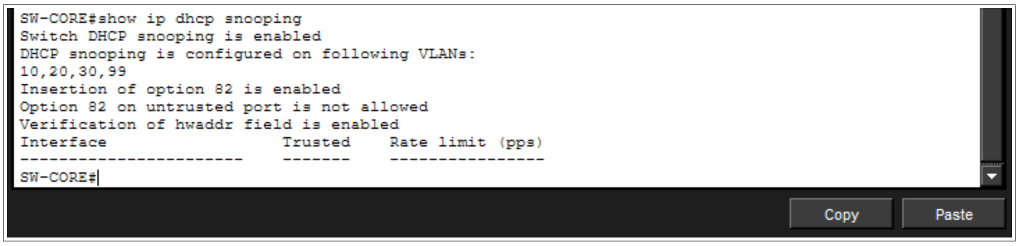
DHCP was configured on Router R1 to automatically assign IP addresses to end devices in the user VLANs. After creating the DHCP pools, DHCP operation was tested from a client workstation.

During testing, DHCP address assignment initially failed. The issue was traced to DHCP snooping behavior/limitations in Packet Tracer, which impacted traffic when used together with the current switching setup. As a result, DHCP snooping was removed to restore correct DHCP functionality in the simulation environment. After this change, DHCP bindings were verified on the router and end-to-end connectivity was tested.



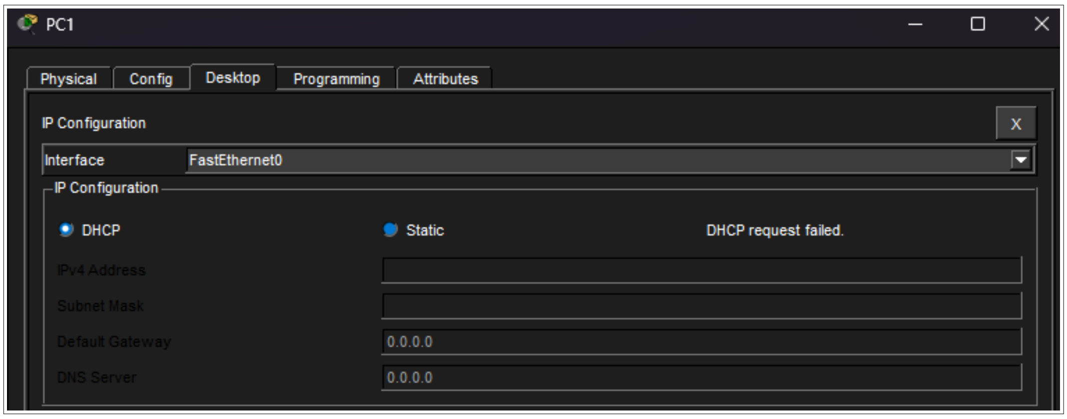
```
R1#show ip dhcp pool

Pool VLAN10_USERS :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 3
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.10.1         192.168.10.1     - 192.168.10.254    0     / 3     / 254

Pool VLAN20_OFFICE :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 3
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.20.1         192.168.20.1     - 192.168.20.254    0     / 3     / 254

Pool VLAN30_GUEST :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 3
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.30.1         192.168.30.1     - 192.168.30.254    0     / 3     / 254
R1#
```

SCREEN #24 - show ip dhcp pool (R1)



```
SW-CORE#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10,20,30,99
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
SW-CORE#
```

SCREEN #25 - show ip dhcp snooping (SW-CORE)



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request failed.

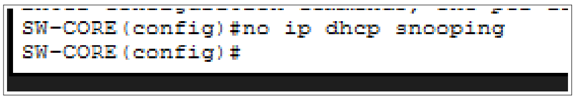
IPv4 Address:

Subnet Mask:

Default Gateway: 0.0.0.0

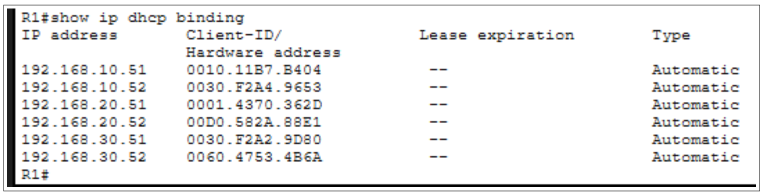
DNS Server: 0.0.0.0

SCREEN #26 - DHCP request failed (PC1)



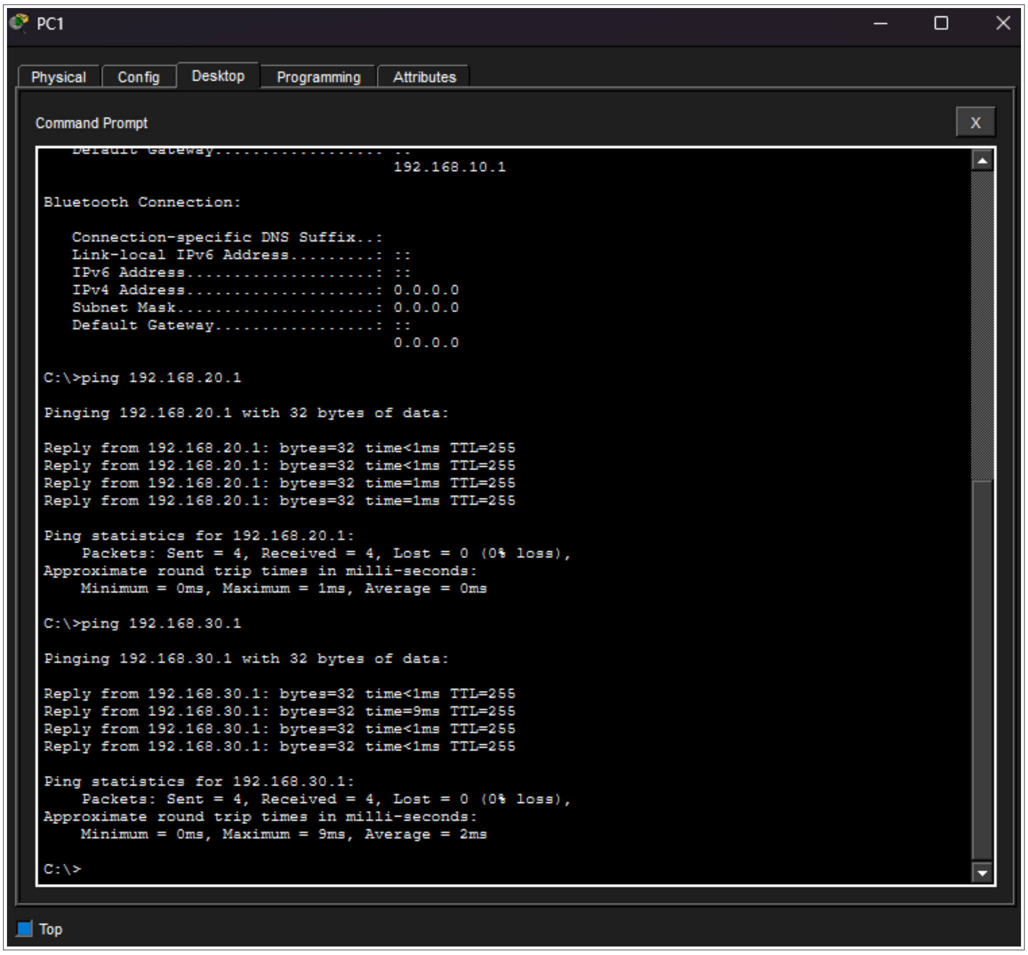
```
SW-CORE(config)#no ip dhcp snooping
SW-CORE(config)#
```

SCREEN #26b - DHCP snooping removal (SW-CORE)



```
R1#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.10.51    0010.11B7.B404           --                     Automatic
192.168.10.52    0030.F2A4.9653           --                     Automatic
192.168.20.51    0001.4370.362D           --                     Automatic
192.168.20.52    00D0.582A.88E1           --                     Automatic
192.168.30.51    0030.F2A2.9D80           --                     Automatic
192.168.30.52    0060.4753.4B6A           --                     Automatic
R1#
```

SCREEN #27 - show ip dhcp binding (R1)



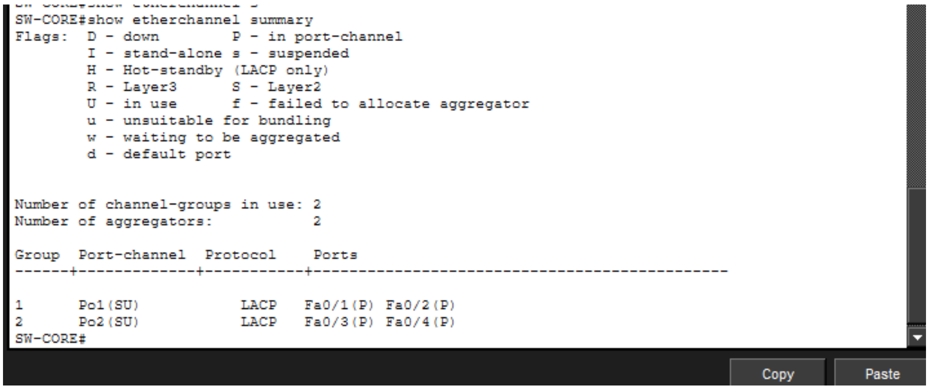
```
   Default Gateway.................: ::
                                     192.168.10.1

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:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time=1ms TTL=255
Reply from 192.168.20.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time=9ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 9ms, Average = 2ms

C:\>
```

SCREEN #28 - inter-VLAN ping tests (PC1)

5.12. EtherChannel Failure Test (Redundancy Verification)

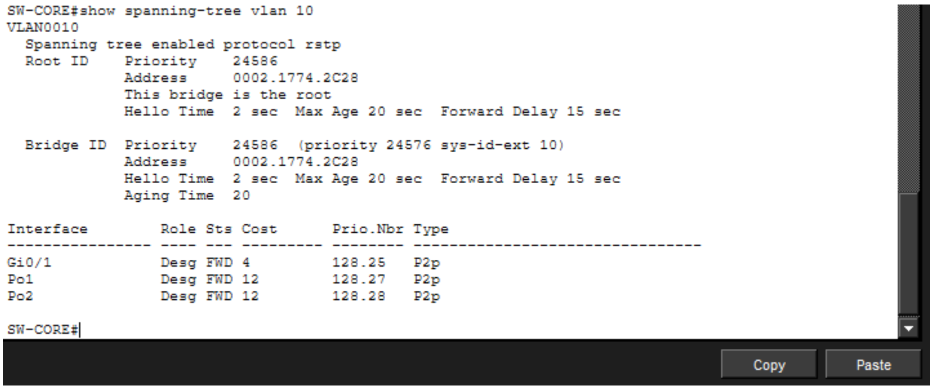
To verify link redundancy, a failure test was performed on the EtherChannel between the core and access switch. One of the physical member interfaces was intentionally brought down to simulate a link failure.

After the failure, EtherChannel status and Spanning Tree operation were checked to confirm that the port-channel remained operational. End-to-end connectivity was then tested to ensure that traffic was still forwarded correctly despite the loss of a physical link.



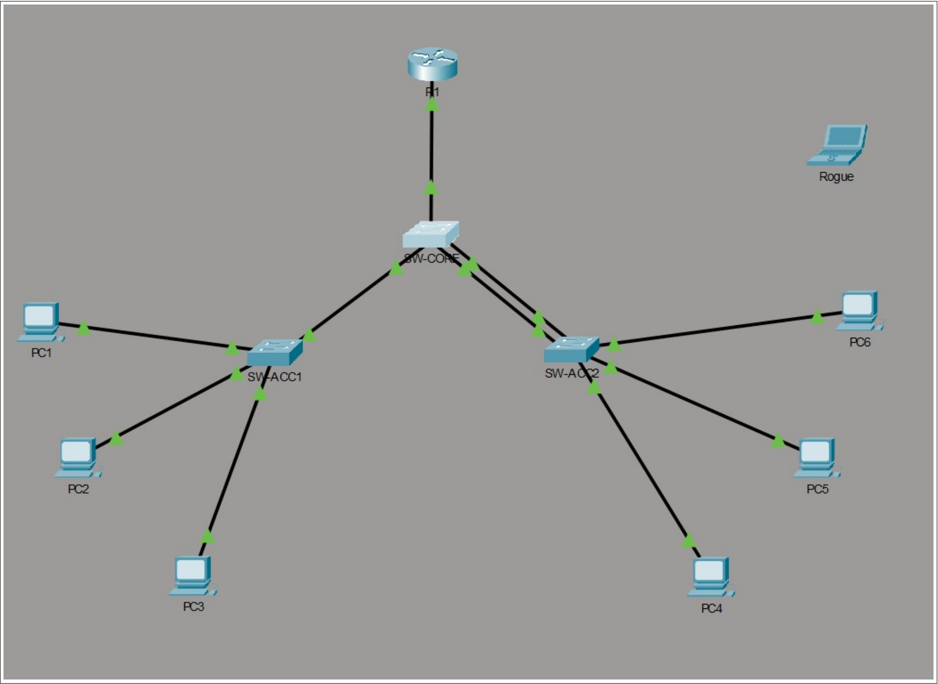
```
SW-CORE#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting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


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+----------------------------------------------

1      Po1(SU)           LACP   Fa0/1(P) Fa0/2(P)
2      Po2(SU)           LACP   Fa0/3(P) Fa0/4(P)
SW-CORE#
```

SCREEN #32 - show etherchannel summary (stable state)

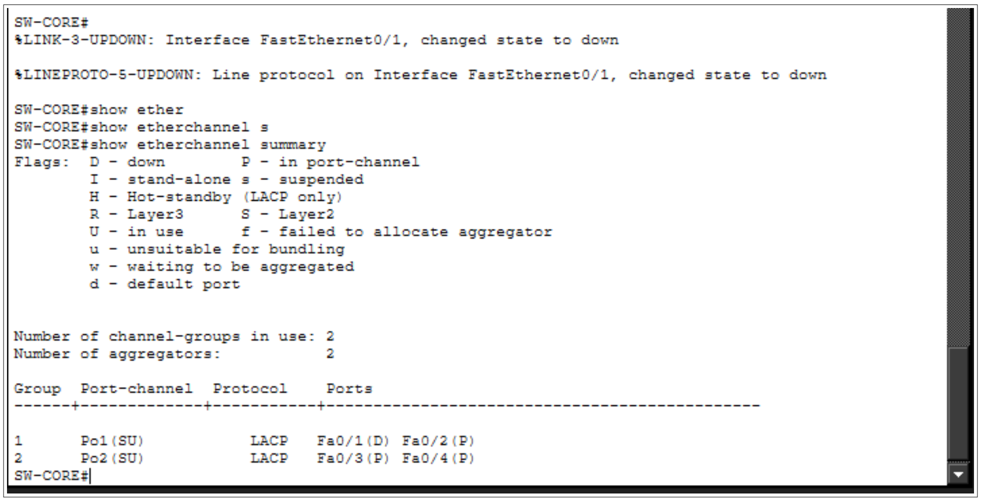


```
SW-CORE#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    24586
             Address     0002.1774.2C28
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24586  (priority 24576 sys-id-ext 10)
             Address     0002.1774.2C28
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Desg FWD 4         128.25   P2p
Po1              Desg FWD 12        128.27   P2p
Po2              Desg FWD 12        128.28   P2p

SW-CORE#
```

SCREEN #33 - show spanning-tree (SW-CORE)

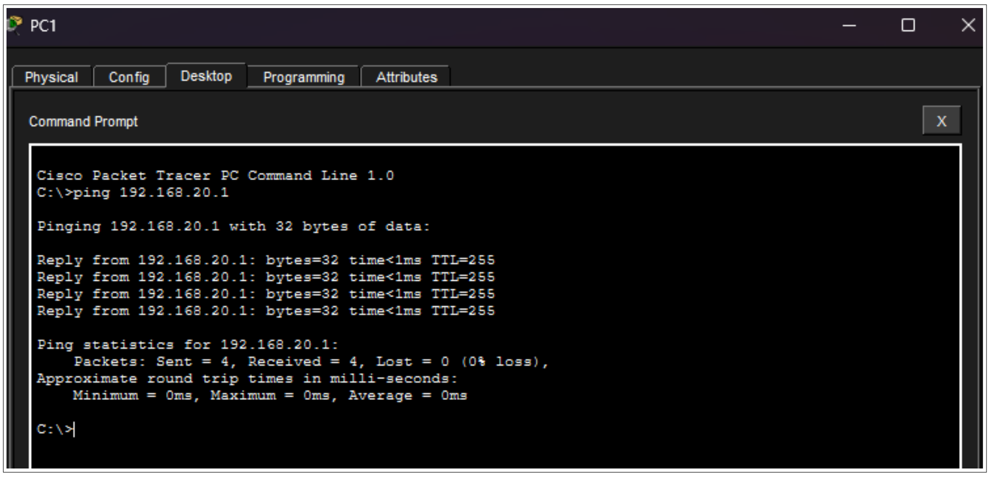


SCREEN #34 - interface malfunction (link down)



```
SW-CORE#
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

SW-CORE#show ether
SW-CORE#show etherchannel s
SW-CORE#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: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+----------------------------------------------

1      Po1(SU)           LACP   Fa0/1(D) Fa0/2(P)
2      Po2(SU)           LACP   Fa0/3(P) Fa0/4(P)
SW-CORE#
```

SCREEN #35 - interface malfunction (second view)



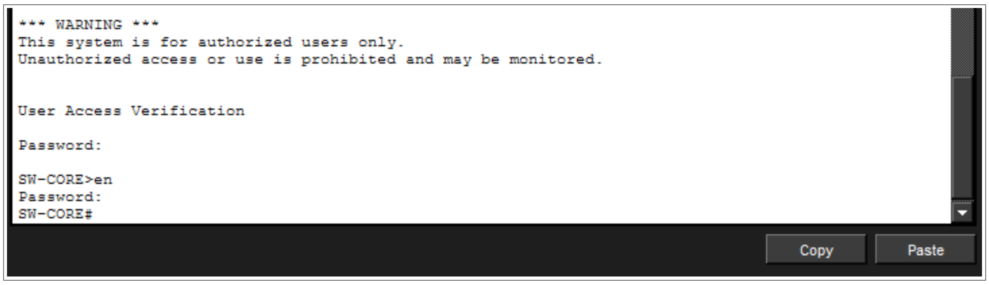
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

SCREEN #36 - connectivity test after failure

5.13. Device Hardening and Secure Management Access (SSH)

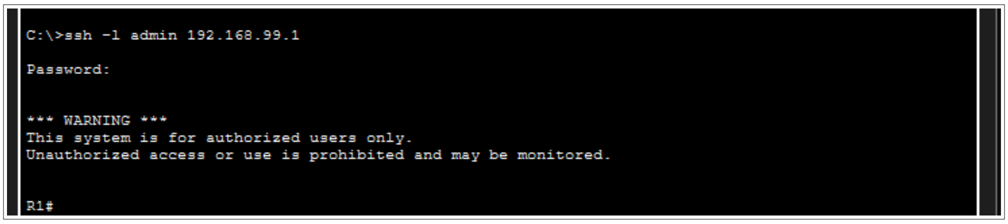
After completing all functional configuration and redundancy testing, basic device hardening was applied to secure administrative access. This step was intentionally performed at the end to avoid interfering with troubleshooting and validation during earlier stages.

The configuration included setting an enable secret, securing console access, adding a warning banner (MOTD), and enabling SSH v2 for remote management while disabling Telnet. SSH access was then verified from a client workstation.



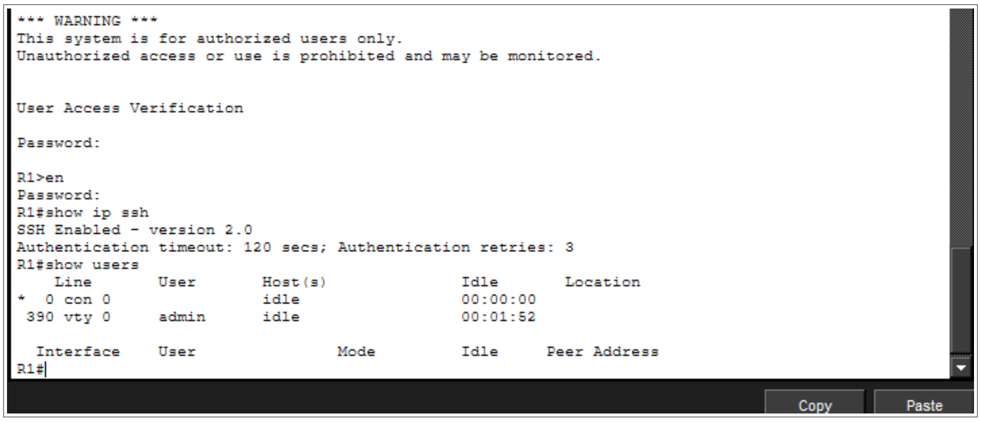
```
*** WARNING ***
This system is for authorized users only.
Unauthorized access or use is prohibited and may be monitored.


User Access Verification

Password:

SW-CORE>en
Password:
SW-CORE#
```

SCREEN #37 - login banner (SW-CORE)



```
C:\>ssh -l admin 192.168.99.1

Password:


*** WARNING ***
This system is for authorized users only.
Unauthorized access or use is prohibited and may be monitored.


R1#
```

SCREEN #38 - SSH access from PC1 to R1



```
*** WARNING ***
This system is for authorized users only.
Unauthorized access or use is prohibited and may be monitored.


User Access Verification

Password:

R1>en
Password:
R1#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
R1#show users
    Line       User       Host(s)              Idle       Location
*  0 con 0                idle                 00:00:00
 390 vty 0     admin      idle                 00:01:52

  Interface    User               Mode         Idle     Peer Address
R1#
```

SCREEN #39 - show ip ssh and show users (R1)

6. Summary

This lab demonstrated the end-to-end deployment of a small campus-style network with multiple VLANs, inter-VLAN routing, and Layer 2 redundancy. The network was built step by step, verified, and adjusted to address configuration issues and simulation limitations encountered during the process.

Key components of the lab included VLAN segmentation, router-on-a-stick (ROAS) inter-VLAN routing, EtherChannel-based link redundancy, and centralized DHCP services. Special attention was given to validation and troubleshooting, reflecting real-world operational scenarios rather than a purely theoretical setup.

Several issues were intentionally documented and resolved, including Packet Tracer limitations, addressing errors, and DHCP-related problems. These scenarios highlight the importance of systematic verification, root cause analysis, and incremental testing when deploying network infrastructure.

Finally, the lab was completed with basic device hardening and secure management access using SSH, ensuring that the network is not only functional but also securely managed. Overall, LAB2 reflects a realistic network implementation workflow, from initial design through troubleshooting and final stabilization.

This lab was designed to simulate real operational challenges commonly encountered in small to medium enterprise networks.

7. Appendix A - Screenshot Checklist

Screen #	Description	Section
1	Network topology	3
2	Physical cabling	5.1
3	Hostname configuration	5.2
4	VLAN creation - show vlan brief (SW-CORE)	5.3
5	EtherChannel summary (SW-CORE)	5.4
6	Trunk interfaces status (SW-CORE)	5.4
7	EtherChannel verification (SW-CORE)	5.4
8	Trunk interfaces status (SW-ACC2)	5.4
9	Final EtherChannel summary (SW-CORE)	5.4
10	Packet Tracer limitation - EtherChannel on router	5.5
11	Corrected network topology	5.6
12	ROAS configuration - subinterfaces	5.7
13	ROAS verification - show ip interface brief	5.7
14	Spanning Tree summary (SW-CORE)	5.8
15	Spanning Tree - VLAN 10	5.8
16	Spanning Tree - VLAN 20	5.8
17	Access port configuration (Fa0/11)	5.9
18	VLAN membership - show vlan brief (SW-ACC1)	5.9
19	Parking VLAN configuration (Fa0/15)	5.9
20	Interface status - show ip interface brief (SW-ACC1)	5.9
21	Management VLAN ping failed (SW-ACC1 to 192.168.99.1)	5.10
22	IP addressing correction on R1	5.10
23	Management VLAN ping successful	5.10
24	DHCP pools configuration (R1)	5.11
25	DHCP snooping status (SW-CORE)	5.11
26	DHCP request failed (PC1)	5.11
26b	DHCP snooping removal (SW-CORE)	5.11
27	DHCP bindings verification (R1)	5.11
28	Inter-VLAN connectivity test (PC1)	5.11
29	ROAS correction - subinterface change	5.7
30	ROAS correction verification	5.7
31	ROAS correction verification (final)	5.7
32	EtherChannel stable state	5.12
33	Spanning Tree after failure test	5.12

8. Appendix B - Device Configuration

8.1. R1 Relevant Configuration

The following excerpt includes only the configuration elements relevant to this lab (ROAS, DHCP, and secure management).

```
hostname R1

enable secret 5 $1$mERr$5.a6P4JqbNiMX01usIfka/

! --- Local admin account ---
username admin privilege 15 secret 5 $1$mERr$AFX/pZT1Lh7NP3Dp3P/qq/

! --- SSH / management settings ---
ip domain-name lab.local
no ip domain-lookup
ip ssh version 2

banner motd ^C
*** WARNING ***
This system is for authorized users only.
Unauthorized access or use is prohibited and may be monitored.
^C

! --- DHCP configuration ---
ip dhcp excluded-address 192.168.10.1 192.168.10.50
ip dhcp excluded-address 192.168.20.1 192.168.20.50
ip dhcp excluded-address 192.168.30.1 192.168.30.50

ip dhcp pool VLAN10_USERS
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 8.8.8.8

ip dhcp pool VLAN20_OFFICE
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 8.8.8.8

ip dhcp pool VLAN30_GUEST
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 8.8.8.8

! --- ROAS (Router-on-a-Stick) trunk to SW-CORE ---
interface GigabitEthernet0/0
 description TRUNK_to_SW-CORE_Gi0/1
 no ip address

interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0

interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0

interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0

interface GigabitEthernet0/0.99
 encapsulation dot1Q 99
 ip address 192.168.99.1 255.255.255.0

interface GigabitEthernet0/0.999
 encapsulation dot1Q 999
 no ip address

! --- Console / VTY lines (SSH only) ---
line con 0
```

```
 password cisco123
 logging synchronous
 login

line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
```

8.2. SW-CORE Relevant Configuration

The following excerpt includes only the configuration elements relevant to this lab (VLAN trunking, EtherChannel, STP, management SVI, and secure access).

Note: DHCP snooping was tested during the lab but later disabled due to Packet Tracer limitations (see Section 5.11).

```
hostname SW-CORE

enable secret 5 $1$mERr$5.a6P4JqbNiMX01usIfka/

! --- Local admin account ---
username admin secret 5 $1$mERr$AFX/pZT1Lh7NP3Dp3P/qq/

! --- SSH / management settings ---
ip domain-name lab.local
no ip domain-lookup
ip ssh version 2

banner motd ^C
*** WARNING ***
This system is for authorized users only.
Unauthorized access or use is prohibited and may be monitored.
^C

! --- STP configuration (CORE as root) ---
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 10,20,30,99 priority 24576
```

```
! --- EtherChannel trunks to access layer ---
interface Port-channel1
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30,99,999
 switchport mode trunk

interface Port-channel2
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30,99,999
 switchport mode trunk

interface FastEthernet0/1
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30,99,999
 switchport mode trunk
 channel-group 1 mode active

interface FastEthernet0/2
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30,99,999
 switchport mode trunk
 channel-group 1 mode active

interface FastEthernet0/3
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30,99,999
 switchport mode trunk
 channel-group 2 mode active

interface FastEthernet0/4
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30,99,999
 switchport mode trunk
 channel-group 2 mode active

! --- Trunk to router (ROAS) ---
interface GigabitEthernet0/1
 description TRUNK_to_R1_G0/0
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30,99,999
 switchport mode trunk

! --- Unused interface after PT limitation ---
interface GigabitEthernet0/2
 description UNUSED_after_PT_limitation
 switchport access vlan 999
 switchport mode access
 shutdown

! --- Management SVI ---
interface Vlan99
 ip address 192.168.99.2 255.255.255.0

ip default-gateway 192.168.99.1

! --- Console / VTY lines (SSH only) ---
line con 0
 password cisco123
 logging synchronous
 login

line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
```

8.3. SW-ACC1 Relevant Configuration

The following excerpt includes only the configuration elements relevant to this lab (access ports, EtherChannel uplink, STP edge protection, management access, and basic hardening).

Note: DHCP snooping was tested during the lab but later disabled due to Packet Tracer limitations.

```
hostname SW-ACC1

enable secret 5 $1$mERr$5.a6P4JqbNiMX01usIfka/

! --- Local admin account ---
username admin secret 5 $1$mERr$AFX/pZT1Lh7NP3Dp3P/qq/
```

```
! --- SSH / management settings ---
ip domain-name lab.local
no ip domain-lookup
ip ssh version 2

banner motd ^C
*** WARNING ***
This system is for authorized users only.
Unauthorized access or use is prohibited and may be monitored.
^C

! --- STP configuration ---
spanning-tree mode rapid-pvst
spanning-tree extend system-id

! --- EtherChannel uplink to CORE ---
interface Port-channel1
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30,99,999
 switchport mode trunk

interface FastEthernet0/1
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30,99,999
 switchport mode trunk
 channel-group 1 mode active

interface FastEthernet0/2
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30,99,999
 switchport mode trunk
 channel-group 1 mode active

! --- Access ports ---
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
```

```
interface FastEthernet0/12
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable

interface FastEthernet0/13
 switchport access vlan 30
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable

interface FastEthernet0/20
 switchport access vlan 10
 switchport mode access

! --- Parking VLAN (unused ports) ---
interface range FastEthernet0/3-10,FastEthernet0/14-19,FastEthernet0/21-24
 switchport access vlan 999
 switchport mode access
 shutdown

! --- Management SVI ---
interface Vlan99
 ip address 192.168.99.11 255.255.255.0

ip default-gateway 192.168.99.1

! --- Console / VTY lines (SSH only) ---
line con 0
 password cisco123
 logging synchronous
 login

line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh#stname SW-ACC1
```

8.4. SW-ACC2 Relevant Configuration

The following excerpt includes only the configuration elements relevant to this lab (access ports, EtherChannel uplink, STP edge protection, management access, and basic hardening).

Note: DHCP snooping was tested during the lab but later disabled due to Packet Tracer limitations.

```
hostname SW-ACC2


enable secret 5 $1$mERr$5.a6P4JqbNiMX01usIfka/


! --- Local admin account ---
username admin secret 5 $1$mERr$AFX/pZT1Lh7NP3Dp3P/qq/


! --- SSH / management settings ---
ip domain-name lab.local
no ip domain-lookup
ip ssh version 2


banner motd ^C
*** WARNING ***
This system is for authorized users only.
Unauthorized access or use is prohibited and may be monitored.
^C


! --- STP configuration ---
spanning-tree mode rapid-pvst
spanning-tree extend system-id


! --- EtherChannel uplink to CORE ---
interface Port-channel2
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30,99,999
 switchport mode trunk


interface FastEthernet0/1
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30,99,999
 switchport mode trunk
 channel-group 2 mode active
```

```
interface FastEthernet0/2
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30,99,999
 switchport mode trunk
 channel-group 2 mode active

! --- Access ports ---
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable

interface FastEthernet0/12
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable

interface FastEthernet0/13
 switchport access vlan 30
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable

! --- Parking VLAN (unused ports) ---
interface range FastEthernet0/3-10,FastEthernet0/14-24
 switchport access vlan 999
 switchport mode access
 shutdown

! --- Management SVI ---
interface Vlan99
 ip address 192.168.99.12 255.255.255.0

ip default-gateway 192.168.99.1

! --- Console / VTY lines (SSH only) ---
line con 0
 password cisco
 logging synchronous
 login

line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
```