Eastern University Sri Lanka

Advanced Networking, Virtualization and Cloud Computing
CS 4163

Practical ICA – (Assessment) 01

Student Name	W.S.M. KULARATHNA
Index Number	PS2616
Registration Number	EU/IS/2018/PHY/016

Date of submission: 28th of MAY 2025

Contents

Table OF Figures

1.0 Network Topology

Create a hierarchical network composed of three layers:

1. Core Layer – Minimum of 2 core routers or switches.
2. Aggregation/Distribution Layer – Minimum of 3 devices.
3. Access Layer – Minimum of 4 access switches.

Requirements:

• Ensure logical separation between layers to support future enhancements (e.g., SDN policy enforcement).

• Use Cisco Packet Tracer to create a network topology diagram including all layers.

• Provide a clear and labeled diagram explaining your topology design.

IP Addressing and VLAN Segmentation

• Develop an IP addressing scheme for your network.

• Configure basic IP addressing on routers and switches.

• Create at least two VLANs (e.g., one for Management/Engineering, another for Guest/Other Users).

• Assign VLANs on access layer switches.

• Configure inter-VLAN routing using a router or Layer 3 switch.

• Use sub-interfaces if required to enable routing between VLANs.

• Provide screenshots of the configuration output.

Submit (git push) your .pkt file along with a document explaining the IP addressing scheme and VLAN configurations.

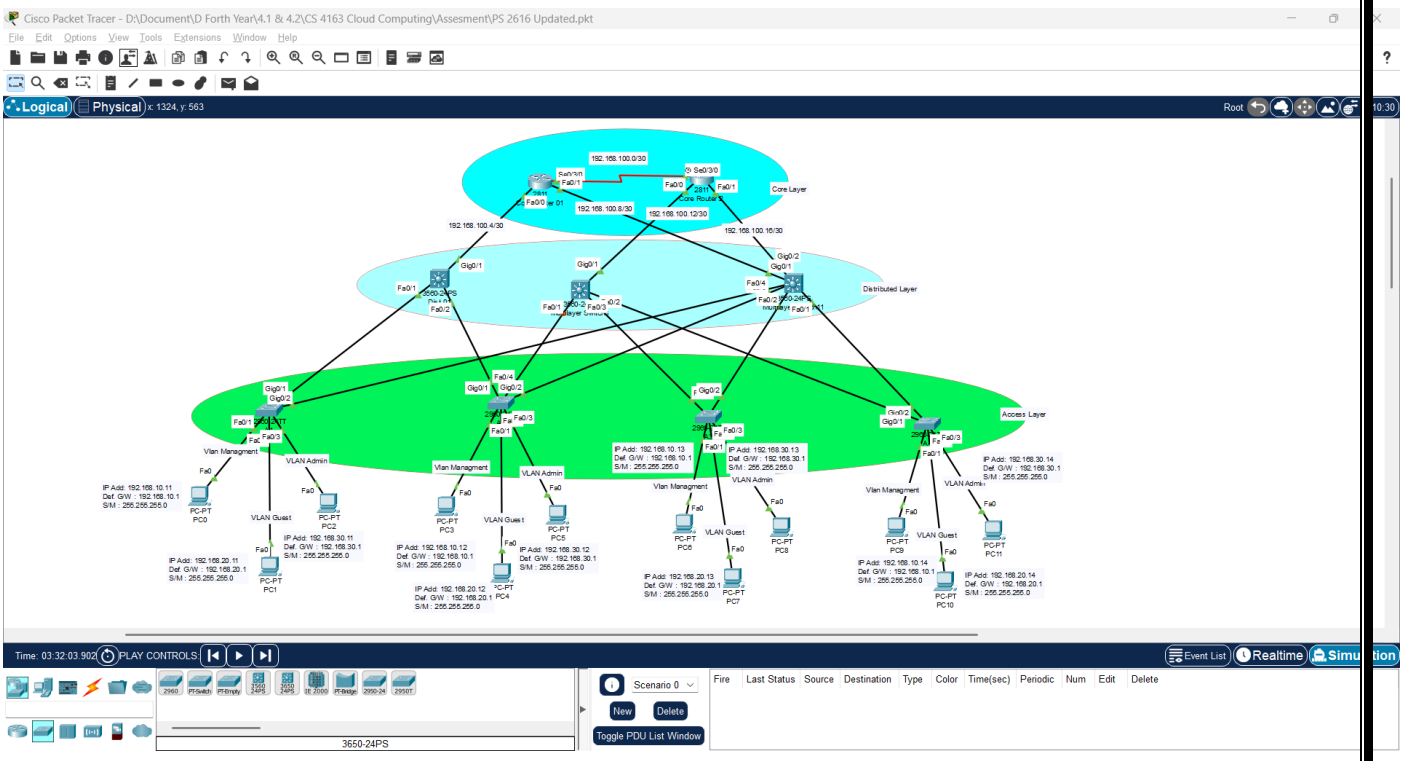

Figure 1Network Topology Diagram

1.1 VLAN Configuration Table

VLAN	Name	Device	Interface	Subnet	IP Address
10	Managment	PC0	Fa0	255.255.255.0	192.168.10.11
10	Managment	PC3	Fa0	255.255.255.1	192.168.10.12
10	Managment	PC6	Fa0	255.255.255.2	192.168.10.13
10	Managment	PC9	Fa0	255.255.255.3	192.168.10.14
20	Guest	PC1	Fa0	255.255.255.3	192.168.20.11
20	Guest	PC4	Fa0	255.255.255.4	192.168.20.12
20	Guest	PC7	Fa0	255.255.255.5	192.168.20.13
20	Guest	PC10	Fa0	255.255.255.6	192.168.20.14
30	Admin	PC2	Fa0	255.255.255.6	192.168.30.11
30	Admin	PC5	Fa0	255.255.255.7	192.168.30.12
30	Admin	PC8	Fa0	255.255.255.8	192.168.30.13
30	Admin	PC11	Fa0	255.255.255.9	192.168.30.14
		Distibuted Layer Switch 01 (Dist 1)	Gig0/1	255.255.252.0	192.168.100.6
		Distibuted Layer Switch 02 (Dist 2)	Gig0/1	255.255.252.0	192.168.100.14
		Distibuted Layer Switch 03 (Dist 3)	Gig0/1	255.255.252.0	192.168.100.10
			Gig0/2	255.255.252.0	192.168.100.18
		Core Layer Router01 (core1)	Fa0/0	255.255.252.0	192.168.100.5
			Fa0/1	255.255.252.0	192.168.100.9
			Se0/3/0	255.255.252.0	192.168.100.1
		Core Layer Router02 (core2)	Fa0/0	255.255.252.0	192.168.100.13
			Fa0/1	255.255.252.0	192.168.100.17

Figure 2VLAN Configuration Table

1.1.1 For A1 (Access layer Switch 01)

```
enable
configure terminal

----VLANs-----

vlan 10
name Management
exit

vlan 20
name Guest
exit

vlan 30
name Admin
exit

vlan 999
name Native
exit
```

----Assign VLANs to access ports---

interface fa0/1
switchport mode access
switchport access vlan 10
exit

interface fa0/2
switchport mode access
switchport access vlan 20
exit

interface fa0/3
switchport mode access
switchport access vlan 30
exit

----Assign VLANs to Trunk ports---

interface range gig0/1 - 2
switchport mode trunk
switchport trunk allowed vlan 10,20,30
switchport trunk native vlan 999

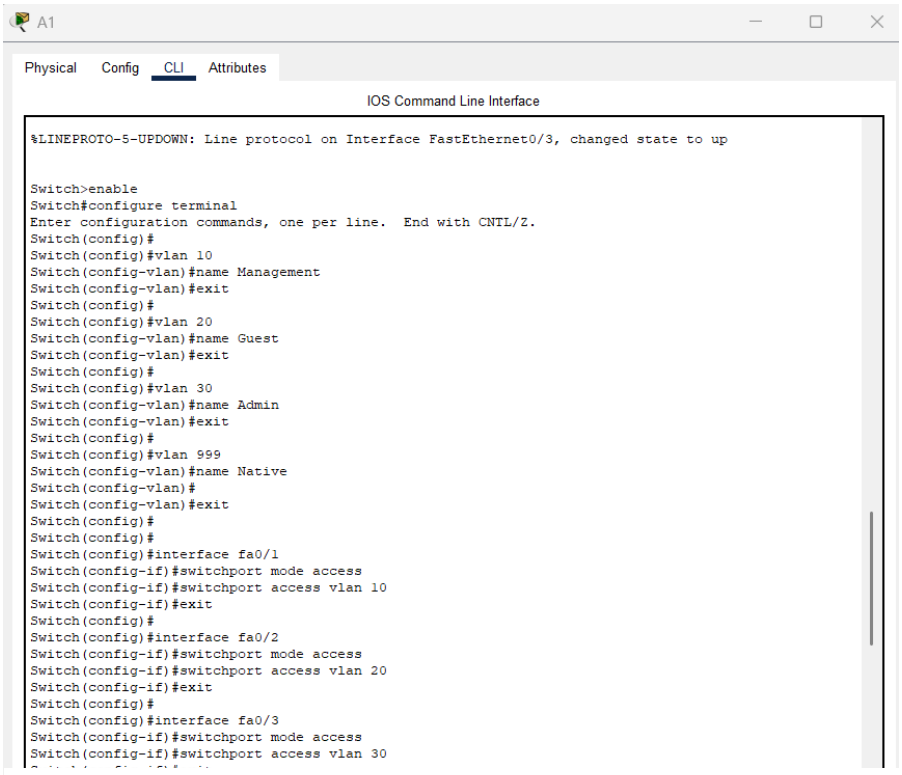

Figure 3Access layer Switch 01 Access port Configuration

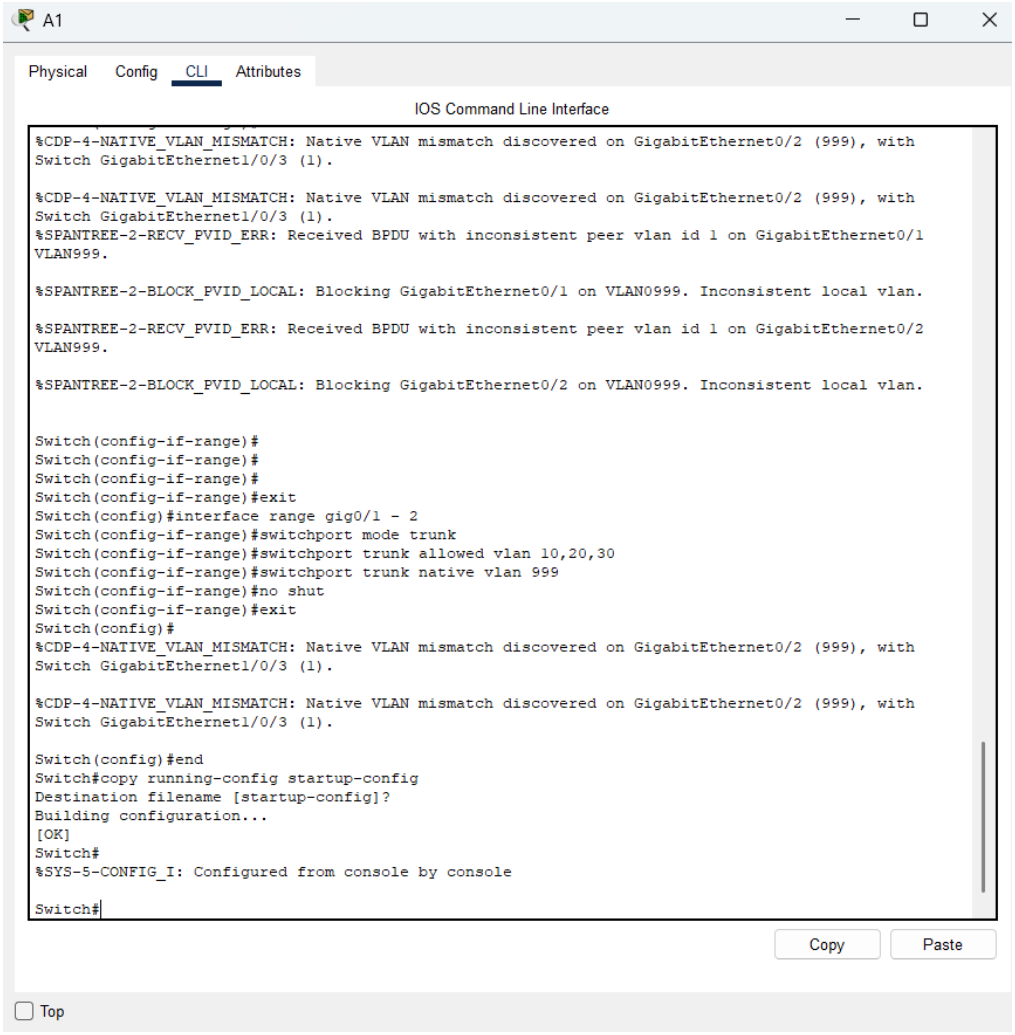

Figure 4Access layer Switch 01 Trunk port Configuration

1.1.2 For A2 (Access layer Switch 02)

enable
configure terminal

----VLANs-----

vlan 10
name Management
exit

vlan 20
name Guest
exit

vlan 30
name Admin
exit

vlan 999
name Native

exit

----Assign VLANs to access ports---

interface fa0/1
switchport mode access
switchport access vlan 10
exit

interface fa0/2
switchport mode access
switchport access vlan 20
exit

interface fa0/3
switchport mode access
switchport access vlan 30
exit

----Assign VLANs to Trunk ports---

interface range gig0/1 - 2
switchport mode trunk
switchport trunk allowed vlan 10,20,30
switchport trunk native vlan 999

interface range fa0/4
switchport mode trunk
switchport trunk allowed vlan 10,20,30
switchport trunk native vlan 999

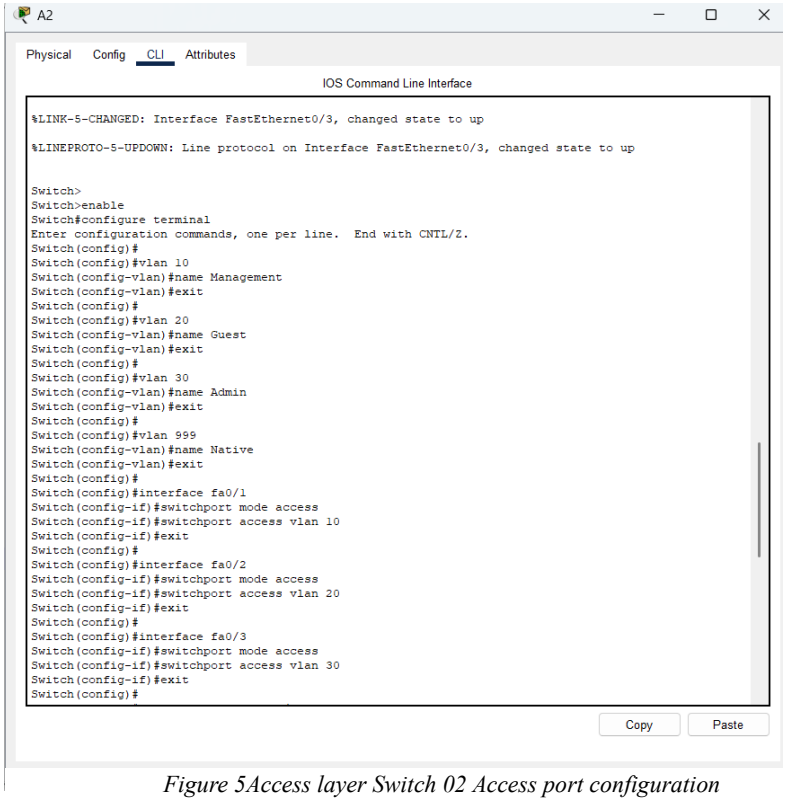

Figure 5Access layer Switch 02 Access port configuration

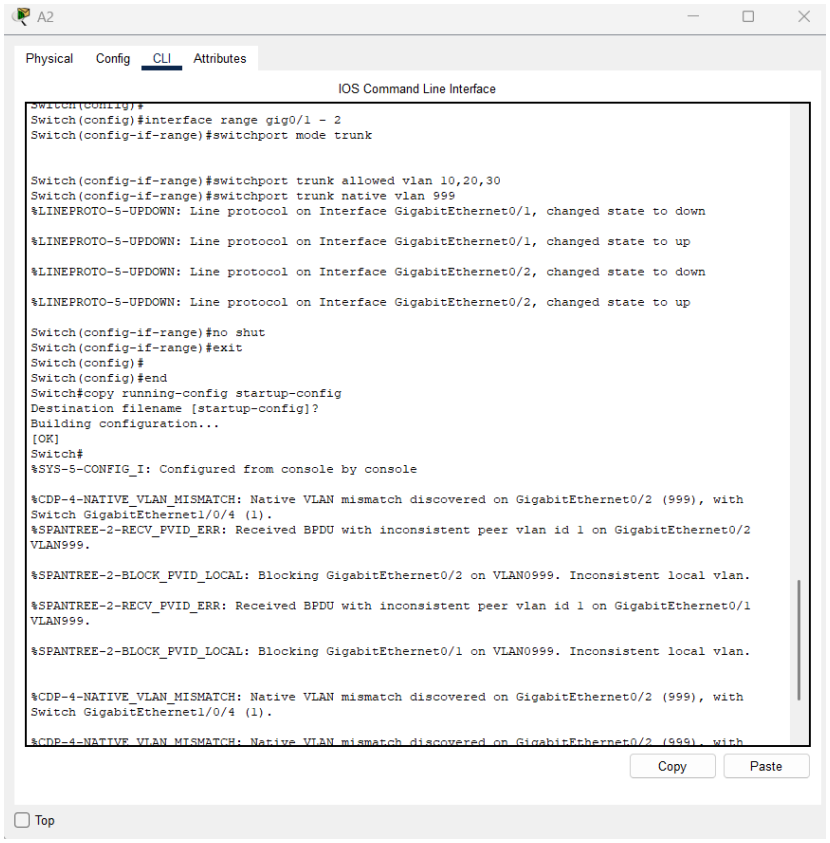

Figure 6Access layer Switch 02 Trunk port Configuration

1.1.3For A3 (Access layer Switch 03)

enable
configure terminal

----VLANs-----

vlan 10
name Management
exit

vlan 20
name Guest
exit

vlan 30
name Admin
exit

vlan 999
name Native
exit

----Assign VLANs to access ports---

interface fa0/1
switchport mode access

switchport access vlan 10
exit

interface fa0/2
switchport mode access
switchport access vlan 20
exit

interface fa0/3
switchport mode access
switchport access vlan 30
exit

----Assign VLANs to Trunk ports---

interface range gig0/1 - 2
switchport mode trunk
switchport trunk allowed vlan 10,20,30
switchport trunk native vlan 999

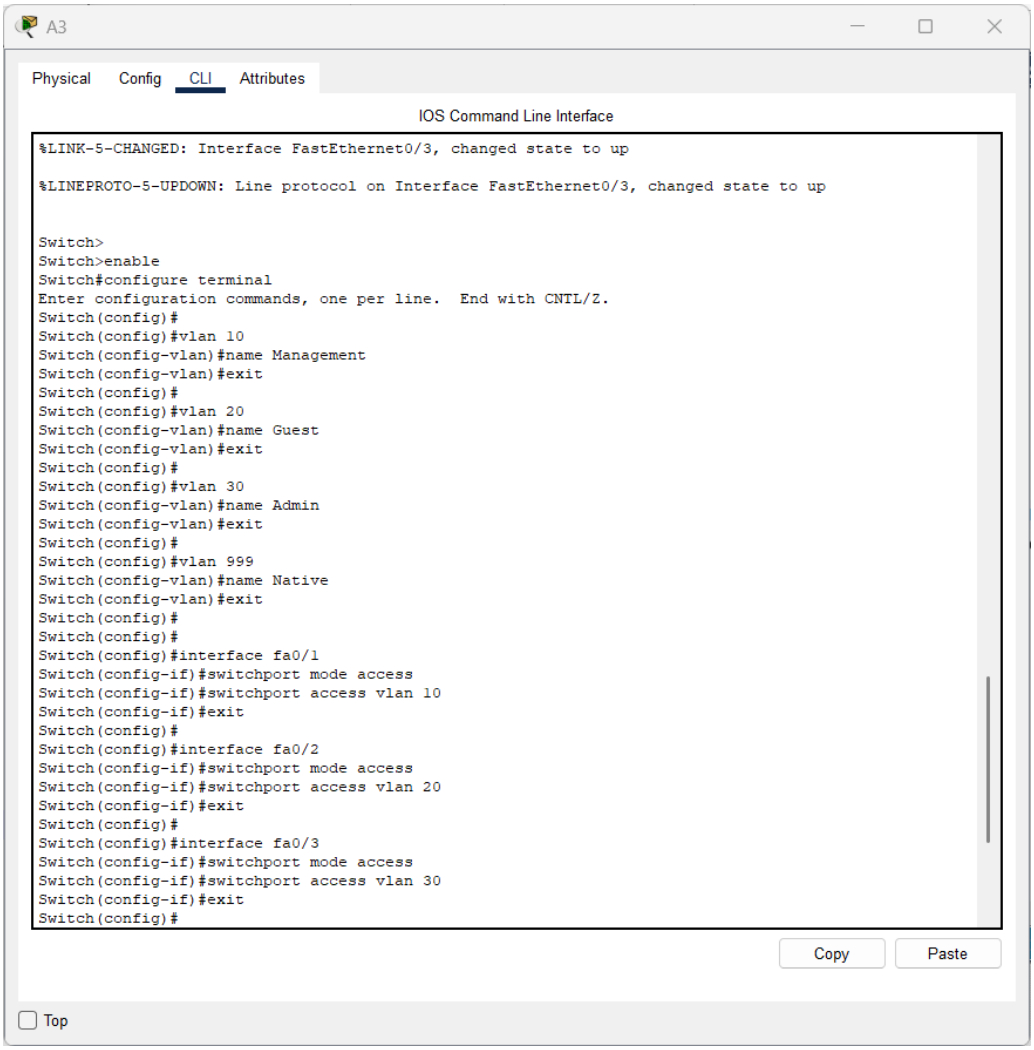

Figure 7Access layer Access Port Configurations Switch 03

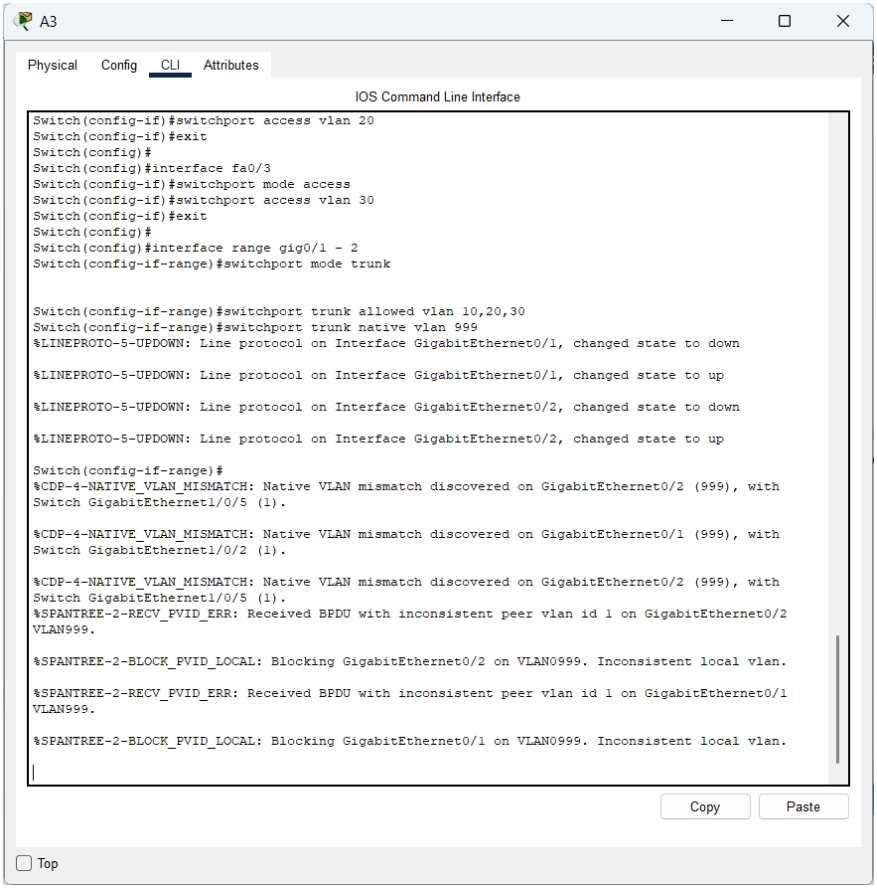

Figure 8 Access layer Trunk port Configurations Switch 03

1.1.4 For A4 (Access layer Switch 04)

enable
configure terminal

----VLANs-----
vlan 10
name Management
exit

vlan 20
name Guest
exit

vlan 30
name Admin
exit

vlan 999
name Native
exit

----Assign VLANs to access ports---

interface fa0/1

switchport mode access
switchport access vlan 10
exit

interface fa0/2
switchport mode access
switchport access vlan 20
exit

interface fa0/3
switchport mode access
switchport access vlan 30
exit

----Assign VLANs to Trunk ports---

interface range gig0/1 - 2
switchport mode trunk
switchport trunk allowed vlan 10,20,30
switchport trunk native vlan 999

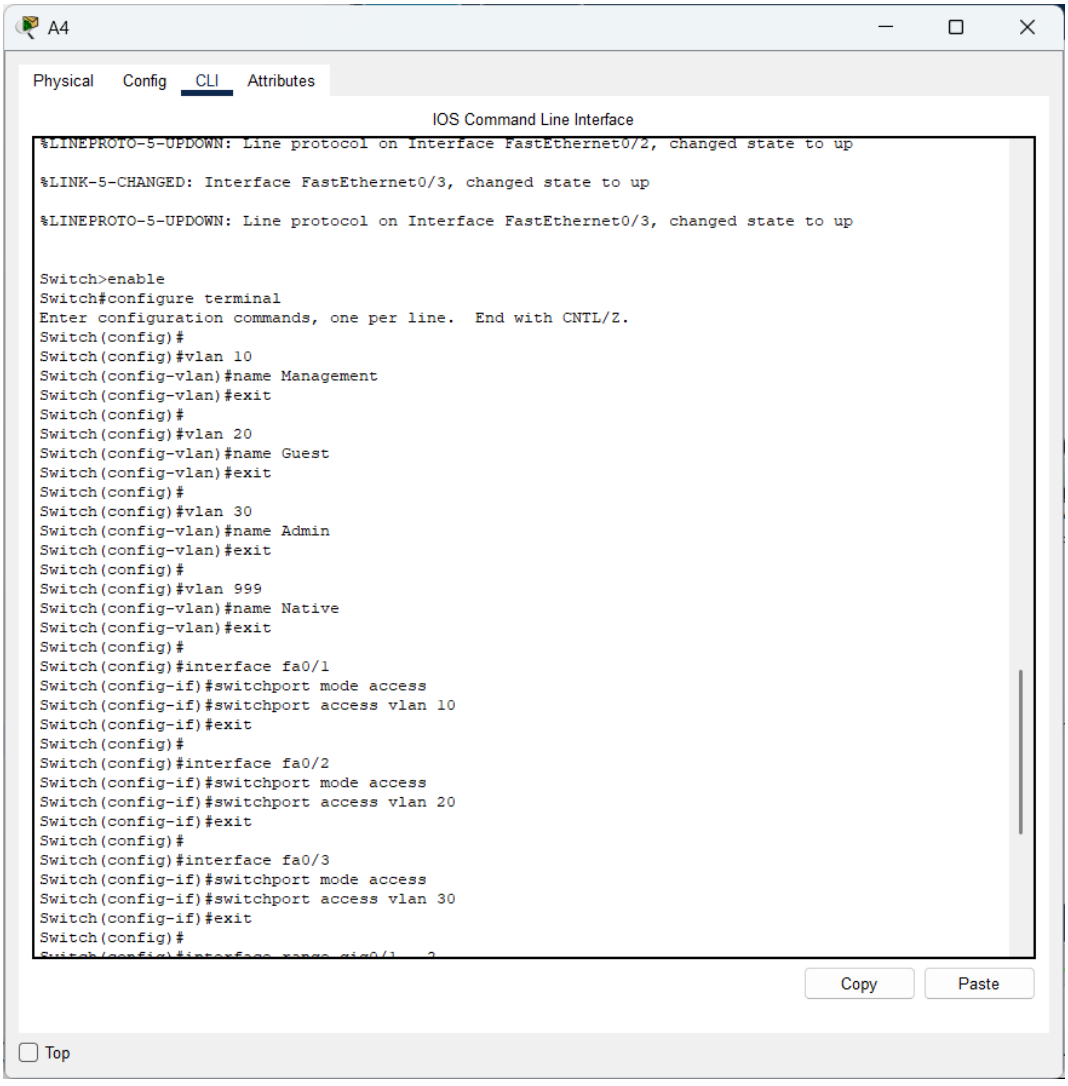

Figure 9Access layer Access port configurations Switch 04

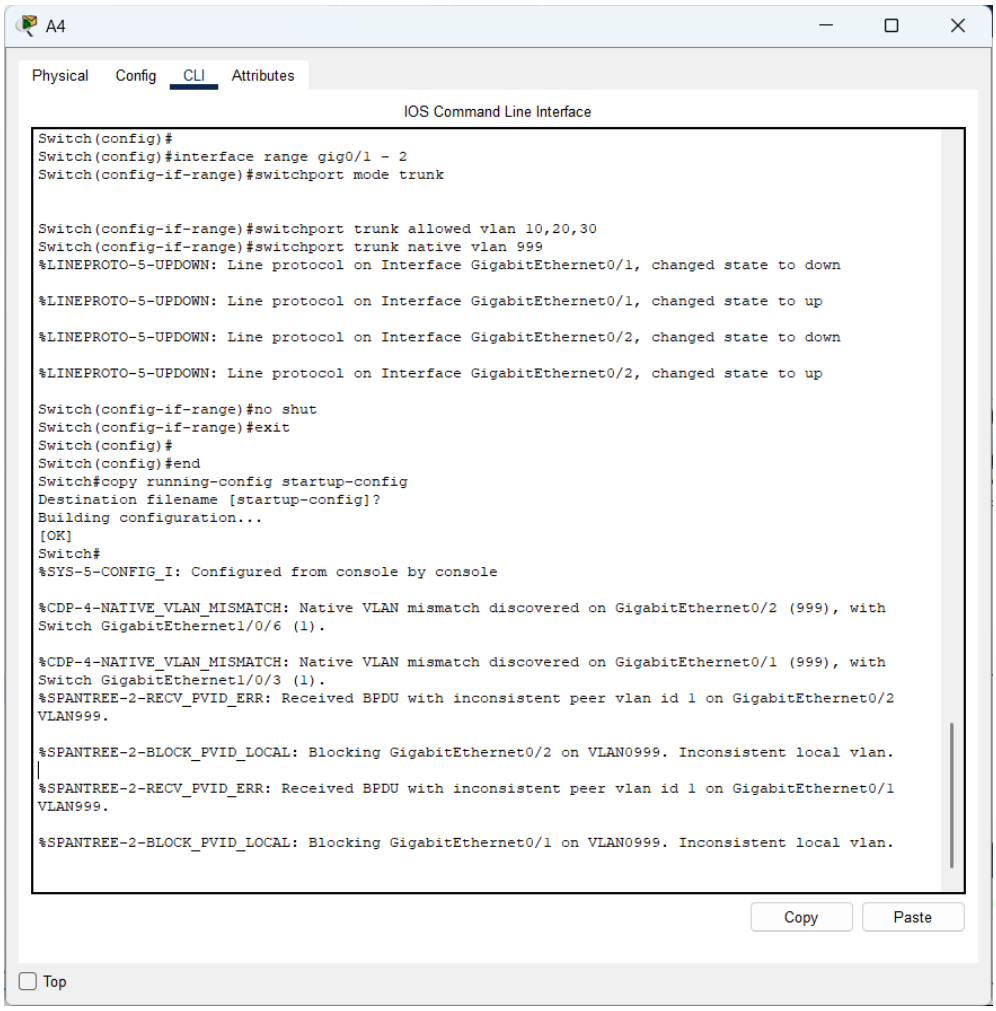

Figure 10 Access layer Trunk port configuration Switch 04

1.1.5 For DIST 01 (Distribution layer Switch 01)

enable
configure terminal

vlan 10
name Management
exit

vlan 20
name Guest
exit

vlan 30
name Admin
exit

vlan 999
name Native
exit

ip routing

--Inter-VLAN routing via SVIs--

interface vlan 10
ip address 192.168.10.1 255.255.255.0
no shutdown
exit

interface vlan 20
ip address 192.168.20.1 255.255.255.0
no shutdown
exit

interface vlan 30
ip address 192.168.30.1 255.255.255.0
no shutdown
exit

---Trunk links to access switches and core Routers---
interface fa0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
switchport trunk native vlan 999
no shutdown
exit

interface fa0/2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
switchport trunk native vlan 999
no shutdown
exit

interface gig0/1
no switchport
ip address 192.168.100.6 255.255.255.252
no shutdown
exit

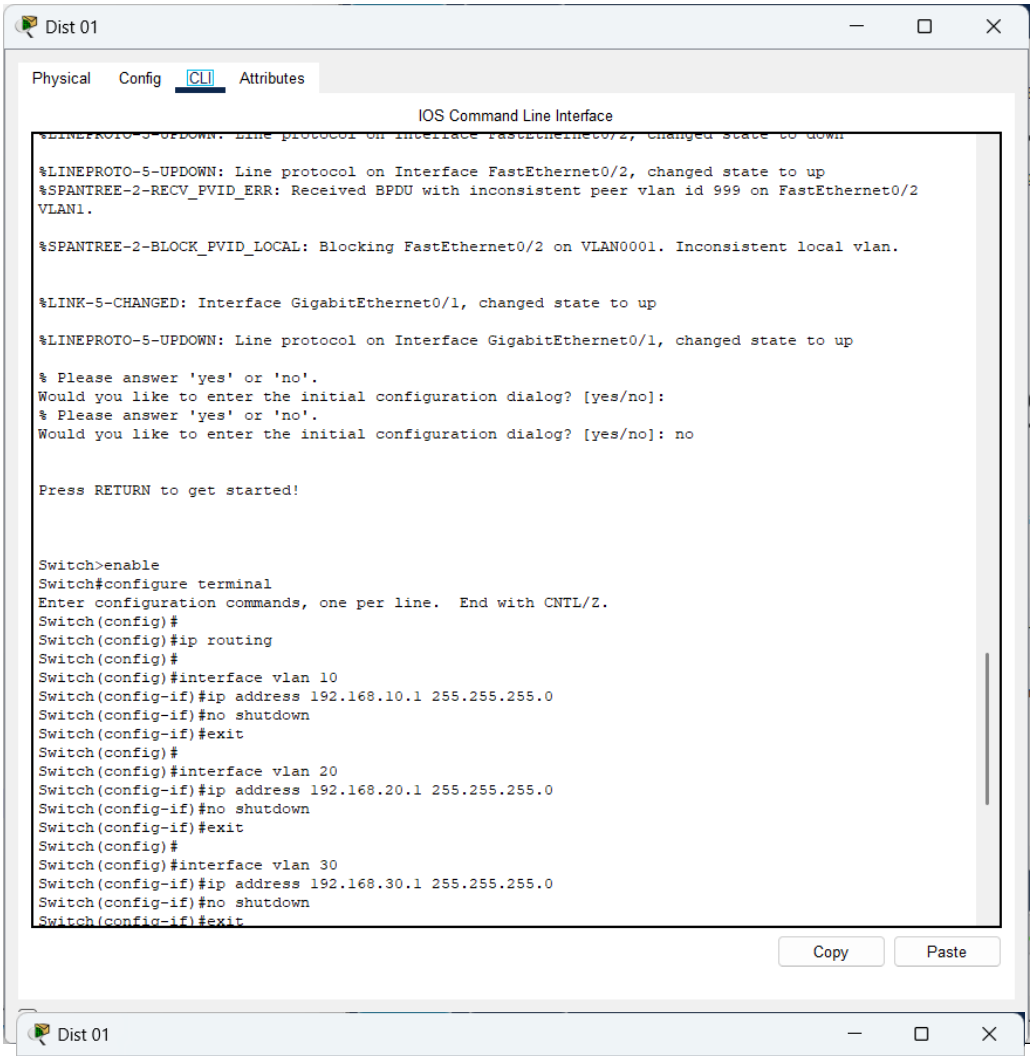

Figure 11 Distribution layer Switch 01 Configuration

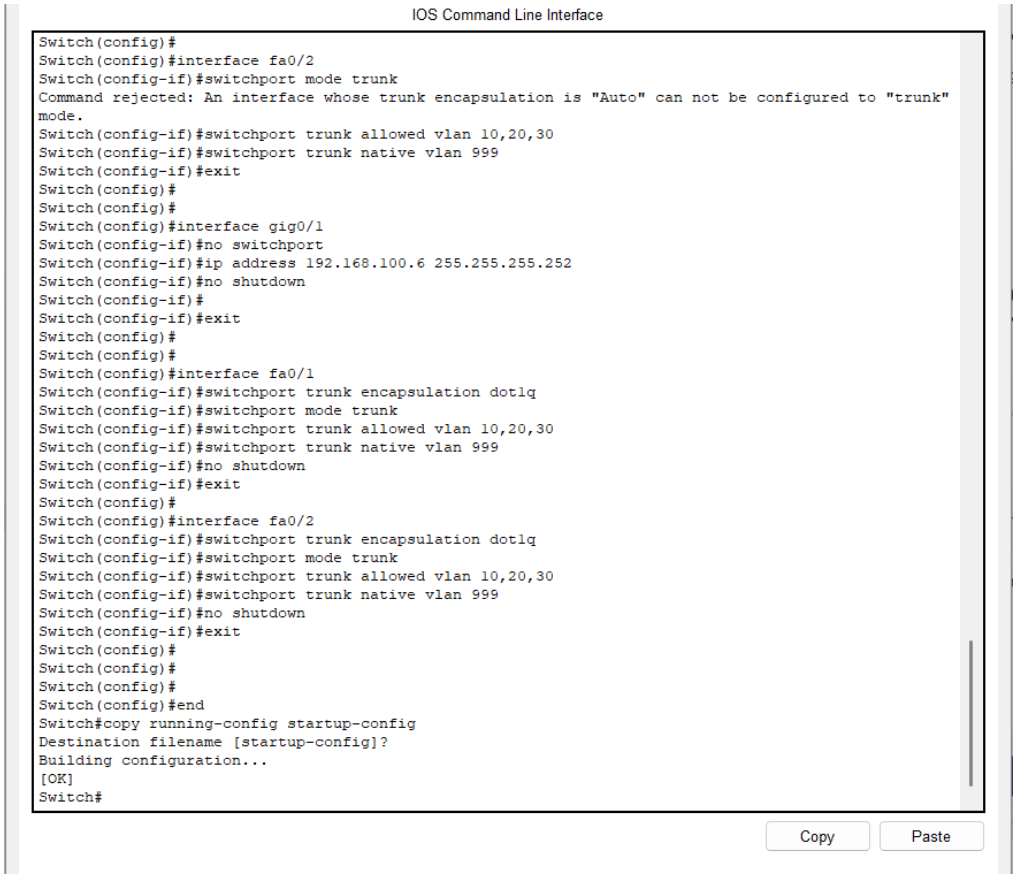

Figure 12Distribution layer Switch 01 Configuration

1.1.6 For DIST 02 (Distribution layer Switch 02)

```
enable
configure terminal

vlan 10
name Management
exit

vlan 20
name Guest
exit

vlan 30
name Admin
exit

vlan 999
name Native
exit


ip routing

--Inter-VLAN routing via SVIs--
interface vlan 10
ip address 192.168.10.1 255.255.255.0
no shutdown
exit

interface vlan 20
ip address 192.168.20.1 255.255.255.0
no shutdown
exit

interface vlan 30
ip address 192.168.30.1 255.255.255.0
no shutdown
exit

---Trunk links to access switches and Routing ---
interface fa0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
switchport trunk native vlan 999
exit

interface fa0/2
switchport trunk encapsulation dot1q
```

switchport mode trunk
switchport trunk allowed vlan 10,20,30
switchport trunk native vlan 999
exit

interface fa0/3
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
switchport trunk native vlan 999
exit

interface gig0/1
no switchport
ip address 192.168.100.14 255.255.255.252
no shutdown

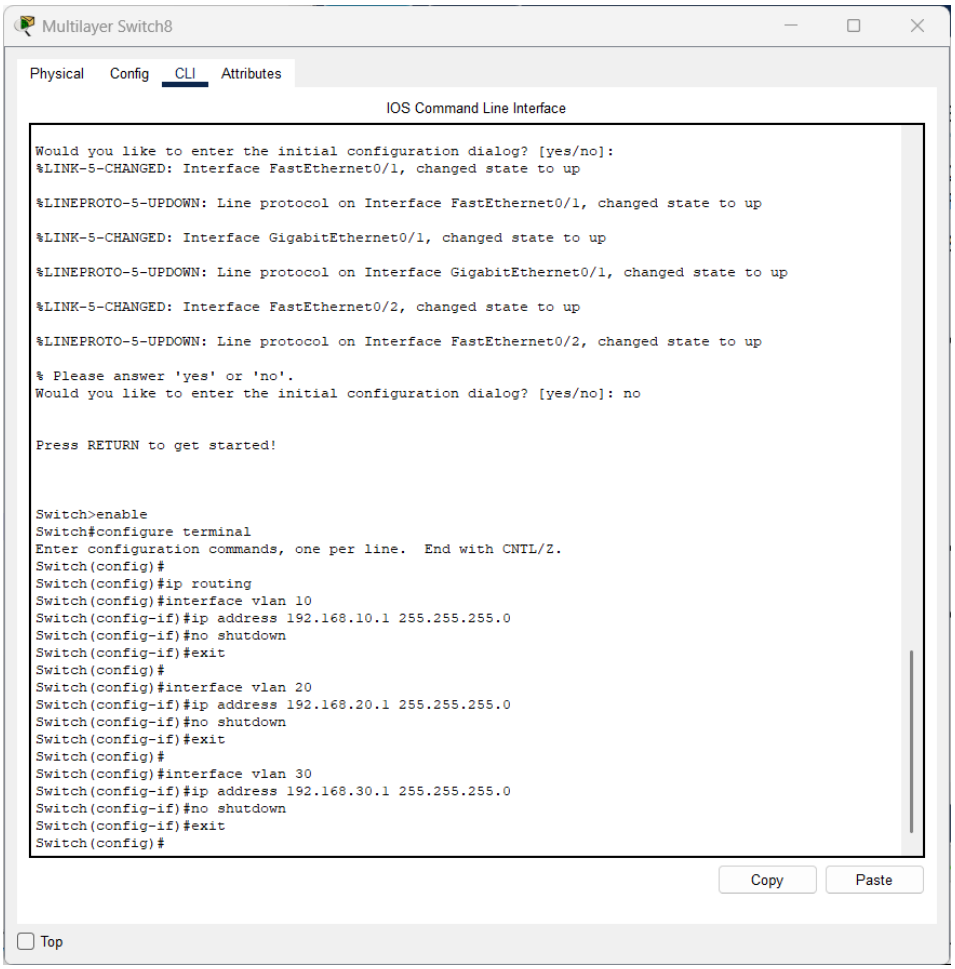

Figure 13Distribution layer Switch 02 Configuration

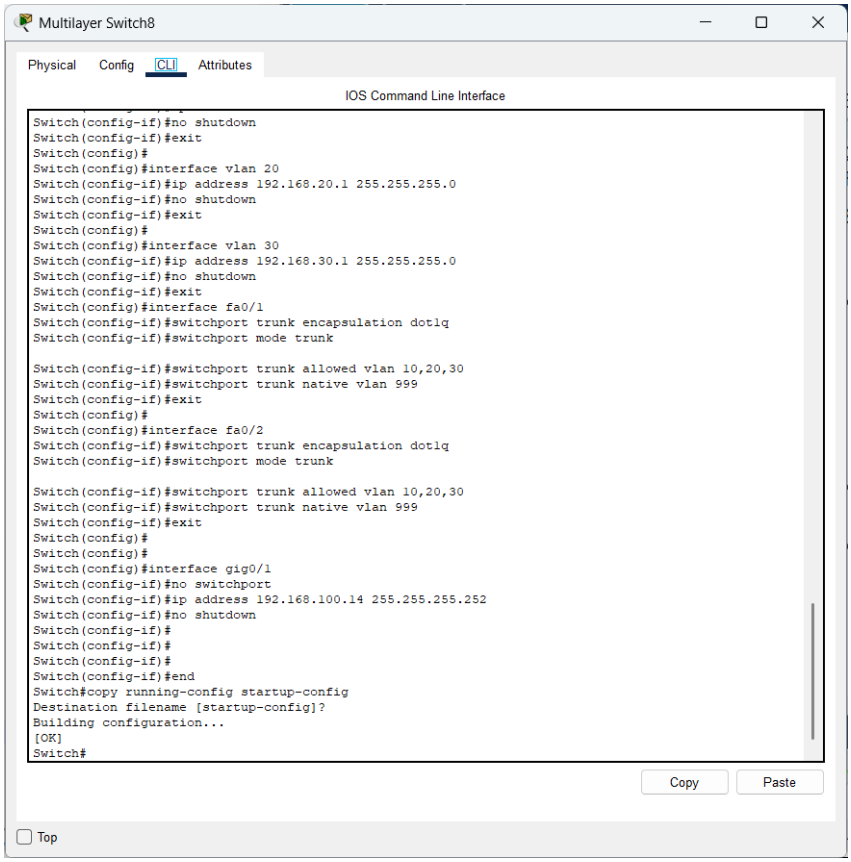

Figure 14Distribution layer Switch 02 Configurations

1.1.7 For DIST 03 (Distribution layer Switch 03)

enable
configure terminal

vlan 10
name Management
exit

vlan 20
name Guest
exit

vlan 30
name Admin
exit

vlan 999
name Native
exit

ip routing

--Inter-VLAN routing via SVIs--

interface vlan 10

ip address 192.168.10.1 255.255.255.0
no shutdown
exit

interface vlan 20
ip address 192.168.20.1 255.255.255.0
no shutdown
exit

interface vlan 30
ip address 192.168.30.1 255.255.255.0
no shutdown
exit

---Trunk links to access switches---
interface fa0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
switchport trunk native vlan 999
exit

interface fa0/2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
switchport trunk native vlan 999
exit

interface fa0/3
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
switchport trunk native vlan 999
exit

interface fa0/4
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
switchport trunk native vlan 999
exit

interface gig0/1
no switchport
ip address 192.168.100.10 255.255.255.252
no shutdown

interface gig0/2

no switchport
ip address 192.168.100.18 255.255.255.252
no shutdown
exit

show interfaces status
show ip interface brief
show vlan brief

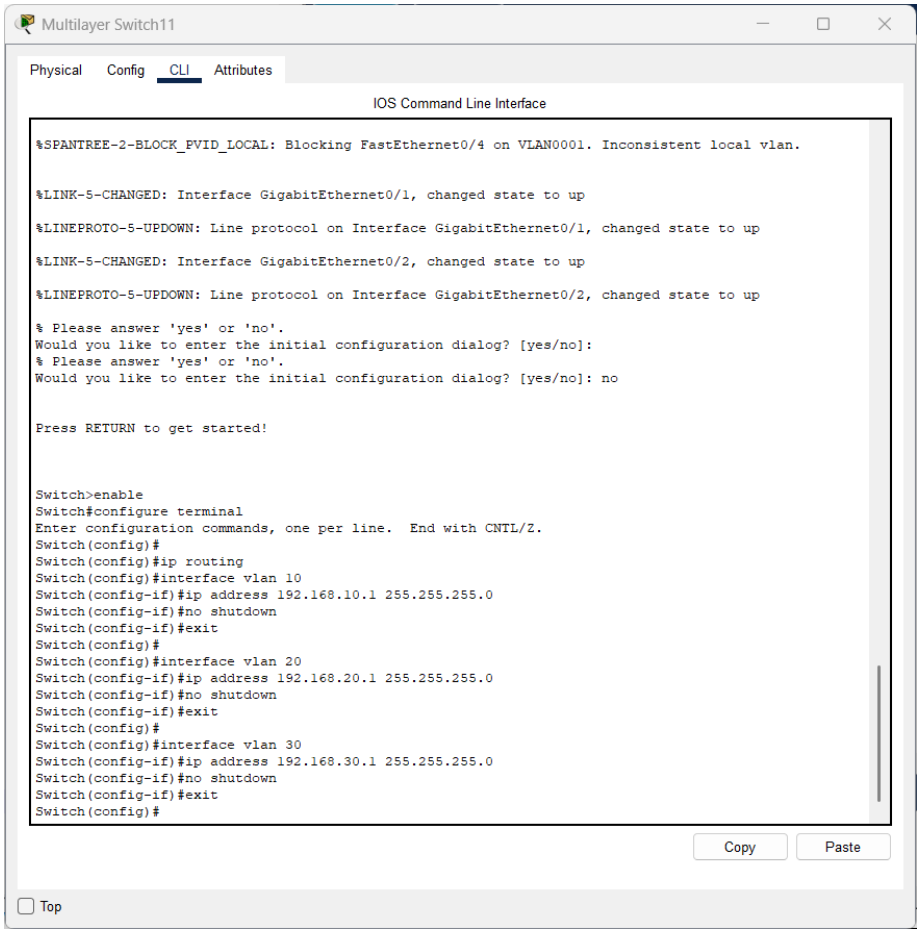

Figure 15Distribution layer Switch 03 Configurations

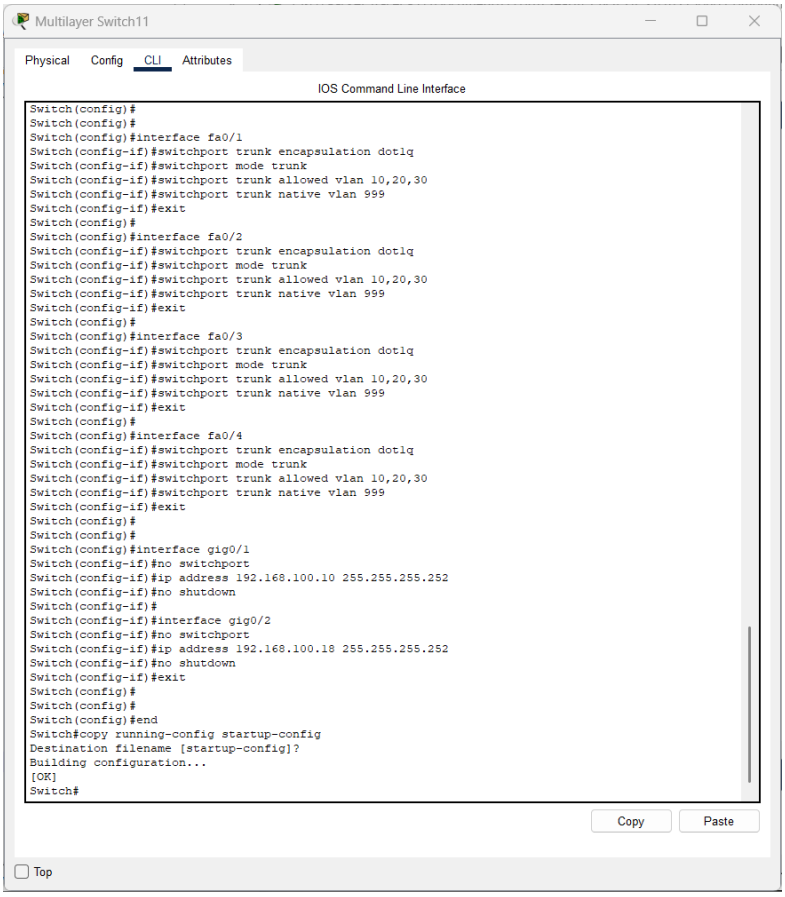

Figure 16 Distribution layer Switch 03 Configurations

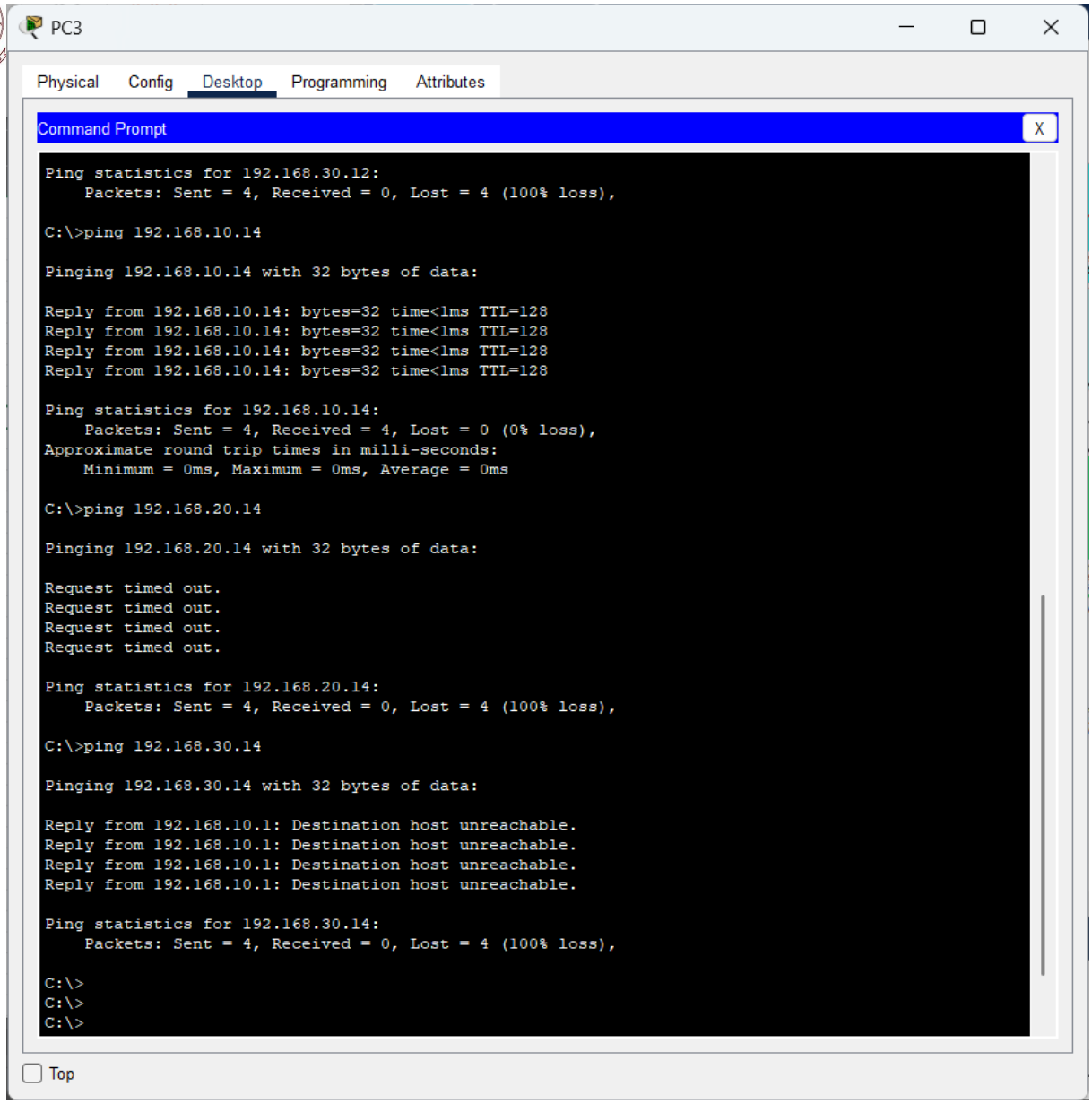

Figure 17 After switch configuration

2.0 Security Policies and ACLs

- Implement and configure Access Control Lists (ACLs) on routers/firewalls to restrict inter VLAN traffic based on your security policies.
- Document each ACL entry with comments and screenshots showing successful traffic filtering.

2.1 ACL Configuration

Allow access to VLAN 10 & VLAN 20. Block VLAN 30. for VLAN 10 (Management)

ip access-list extended VLAN10_ACCESS

deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
permit ip 192.168.10.0 0.0.0.255 192.168.0.0 0.0.255.255
exit

Allow only local access. Block access to VLAN 10 & VLAN 30. (for VLAN 20 (Guest))
ip access-list extended VLAN20_ACCESS

deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
permit ip 192.168.20.0 0.0.0.255 192.168.20.0 0.0.0.255
exit

interface vlan 10
ip access-group VLAN10_ACCESS in
exit

interface vlan 20
ip access-group VLAN20_ACCESS in
exit

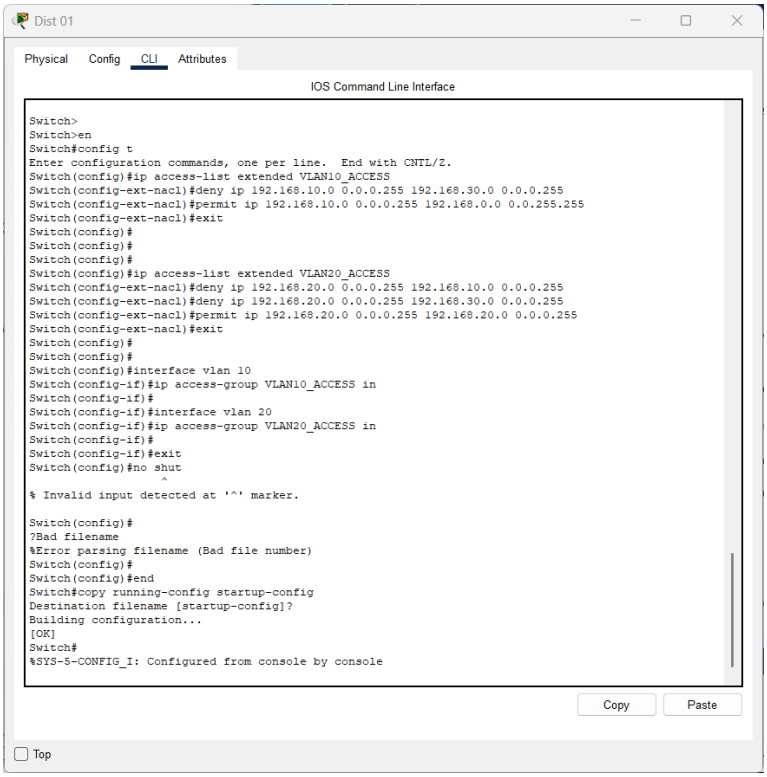

Figure 18 ACL Configurations

After Apply ACL

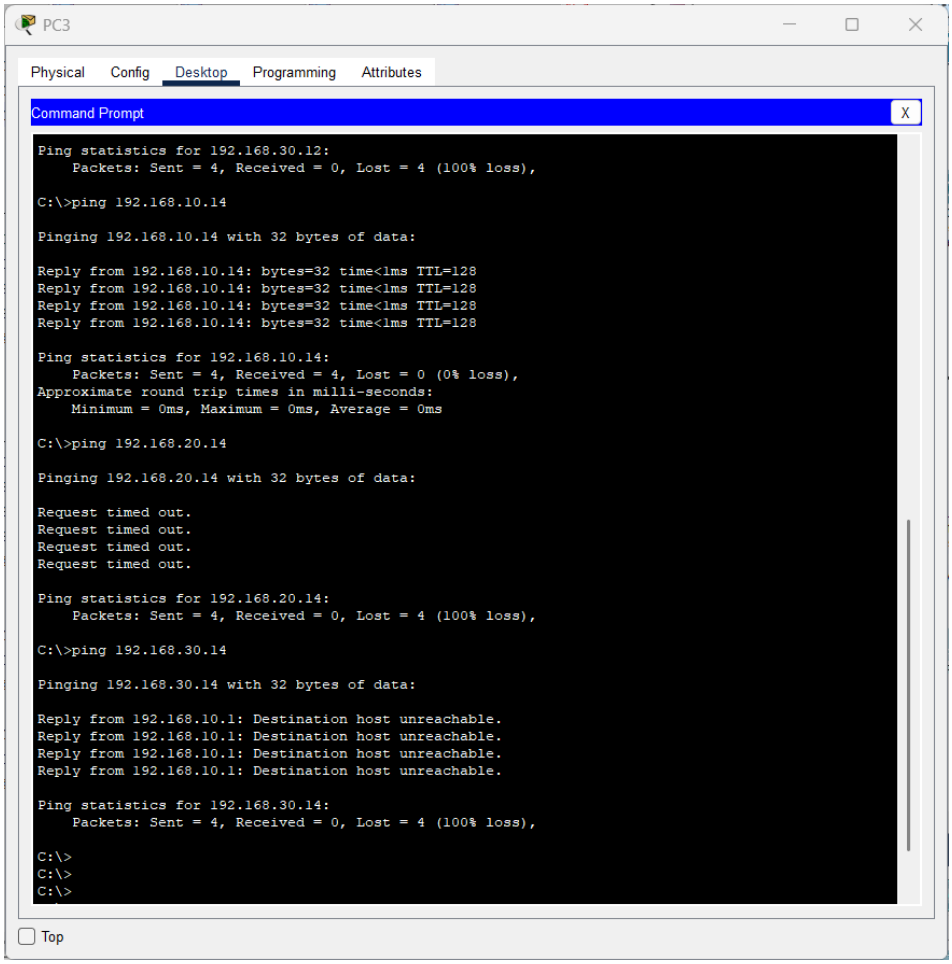

Figure 19 After ACL Configuration for VLAN 20 (Guest)

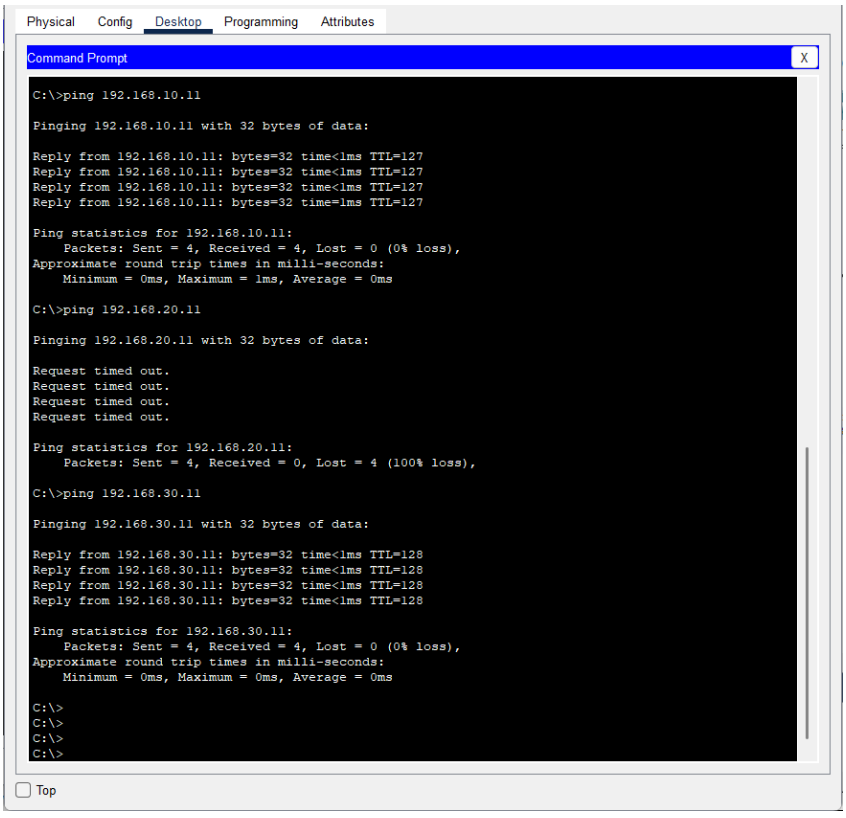

Figure 20 After ACL Configuration for VLAN 10 (Management)

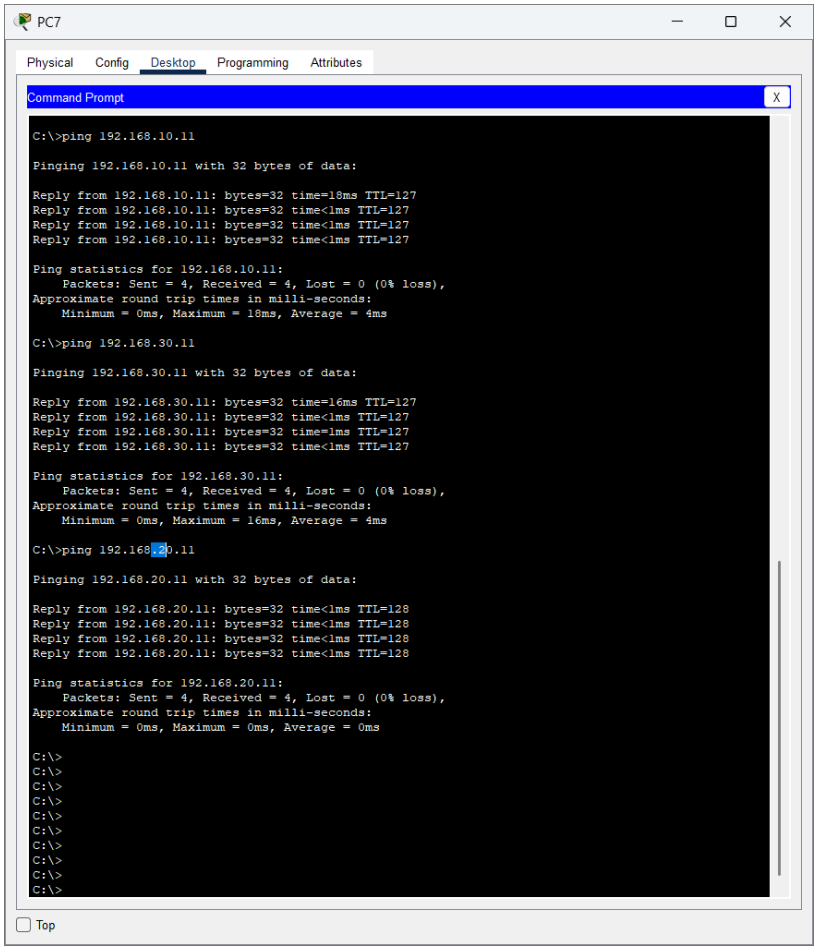

Figure 21 After ACL Configuration for VLAN 30 (Admin)

3.0 Failover and Redundancy

- Implement a redundancy protocol such as HSRP, VRRP, or a dynamic routing protocol on
- routers/switches for automatic failover.
- Simulate a network device or link failure and show how traffic is automatically rerouted.
- Document how the failover mechanism works with:

  o Detailed notes
  o Simulation captures/screenshots of before and after the failure
  o Clear comments on the behaviour observed

3.1 What is the Failover?

Failover is a backup operational mode in which the functions of a system component are assumed by a secondary component when the primary becomes unavailable. An organization can fail over either after failure or during scheduled down time. (Contributor, 2023)

3.2 What is the network redundancy?

Network redundancy is the process of **providing multiple paths for traffic** so that data can keep flowing even in the event of a failure. Put simply: more redundancy equals more reliability. It also helps with distributed site management. The idea is that if one device fails, another can automatically take over. By adding a little bit of complexity, we reduce the probability that a failure will take the network down. (Dooley, 2024)

3.3 What is the HSRP (Host Standby Router Protocol)?

HSRP is the cisco proprietary Protocol designed to provide network redundancy for IP network. It ensures that Traffic Immediately and transparently recovers from first hop Failures in network edge devices or access circuits. (HSRP (Hot Standby Routing Protocol), n.d.)

HSRP allows multiple routers to work together to present the illusion of a single virtual router to the hosts on the LAN. This set of routers is known as an HSRP group or a standby group. A single router, elected from the group, is responsible for forwarding the packets sent to the virtual router. This router is known as the Active router. Another router is elected as the Standby router. If the Active router fails, the Standby router takes over the packet-forwarding duties (Understand the Hot Standby Router Protocol Features and Functionality, 2023)

3.4 What are the HSRP States?

- ✓ Initial State: - when the interface Goes in up state
- ✓ Learn State: -The router is trying to learn Virtual IP Address
- ✓ Listen State: - The router knowns Virtual IP address and listened from Active and Standby routers
- ✓ Speak State: -The router is sending and participating in the election to become the active router
- ✓ Standby State: - This is the router which will l become the active routers and continuously sending message to active router (Kareemoddin, 2016)

3.5 Why Use HSRP Instead of Static Gateway?

Static Gateway	**HSRP**
Single point of failure	No single point of failure
Manual reconfiguration	Automatic failover
Downtime likely	Minimal to no downtime

3.6 HSRP Implementation

```
on Core1
interface Vlan10
 ip address 192.168.10.2 255.255.255.0
 standby 10 ip 192.168.10.1
 standby 10 priority 110
 standby 10 preempt
 no shutdown
 exit

interface Vlan20
 ip address 192.168.20.2 255.255.255.0
 standby 20 ip 192.168.20.1
```

```
 standby 20 priority 110
 standby 20 preempt
 no shutdown
 exit

interface Vlan30
 ip address 192.168.30.2 255.255.255.0
 standby 30 ip 192.168.30.1
 standby 30 priority 110
 standby 30 preempt
 no shutdown
 exit

on Core2
interface Vlan10
 ip address 192.168.10.3 255.255.255.0
 standby 10 ip 192.168.10.1
 standby 10 priority 100
 standby 10 preempt
 no shutdown
 exit

interface Vlan20
 ip address 192.168.20.3 255.255.255.0
 standby 20 ip 192.168.20.1
 standby 20 priority 100
 standby 20 preempt
 no shutdown
 exit

interface Vlan30
 ip address 192.168.30.3 255.255.255.0
 standby 30 ip 192.168.30.1
 standby 30 priority 100
 standby 30 preempt
 no shutdown
 exit
```

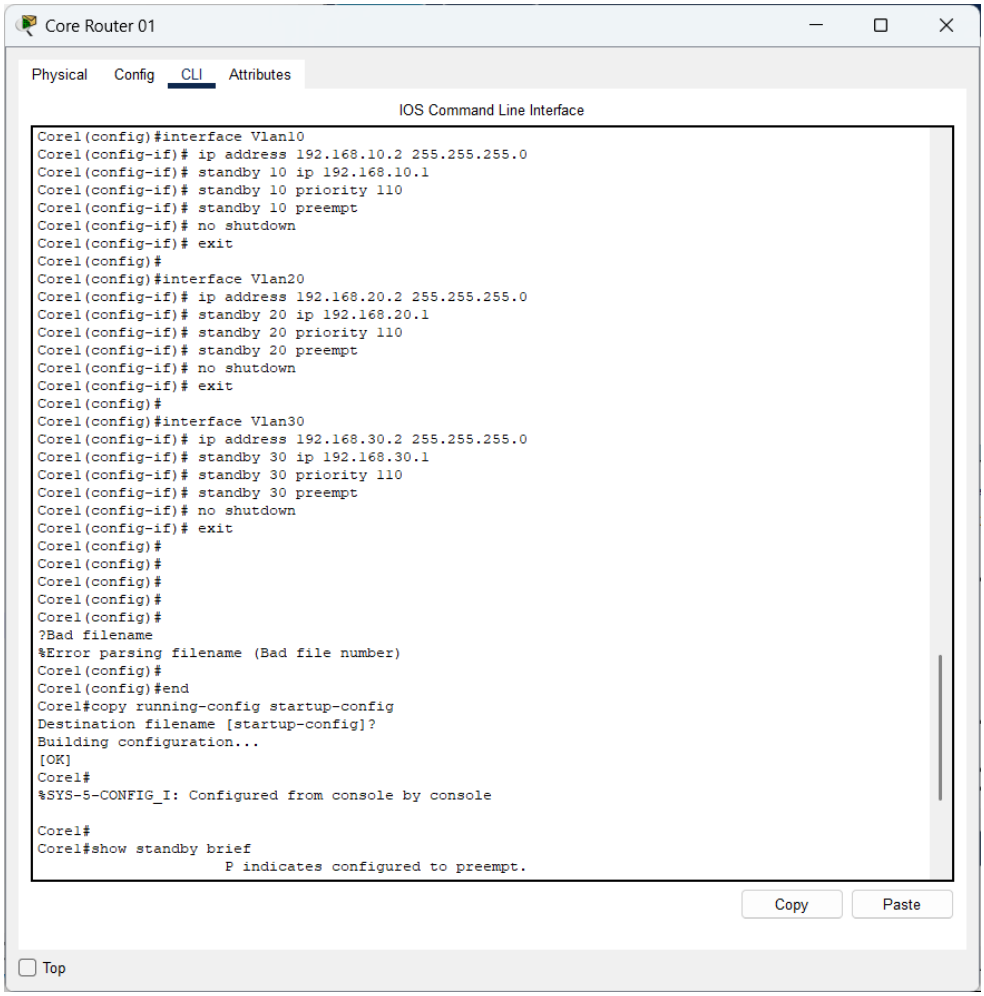

Figure 22 HSRP Implementation for Route01 (core01)

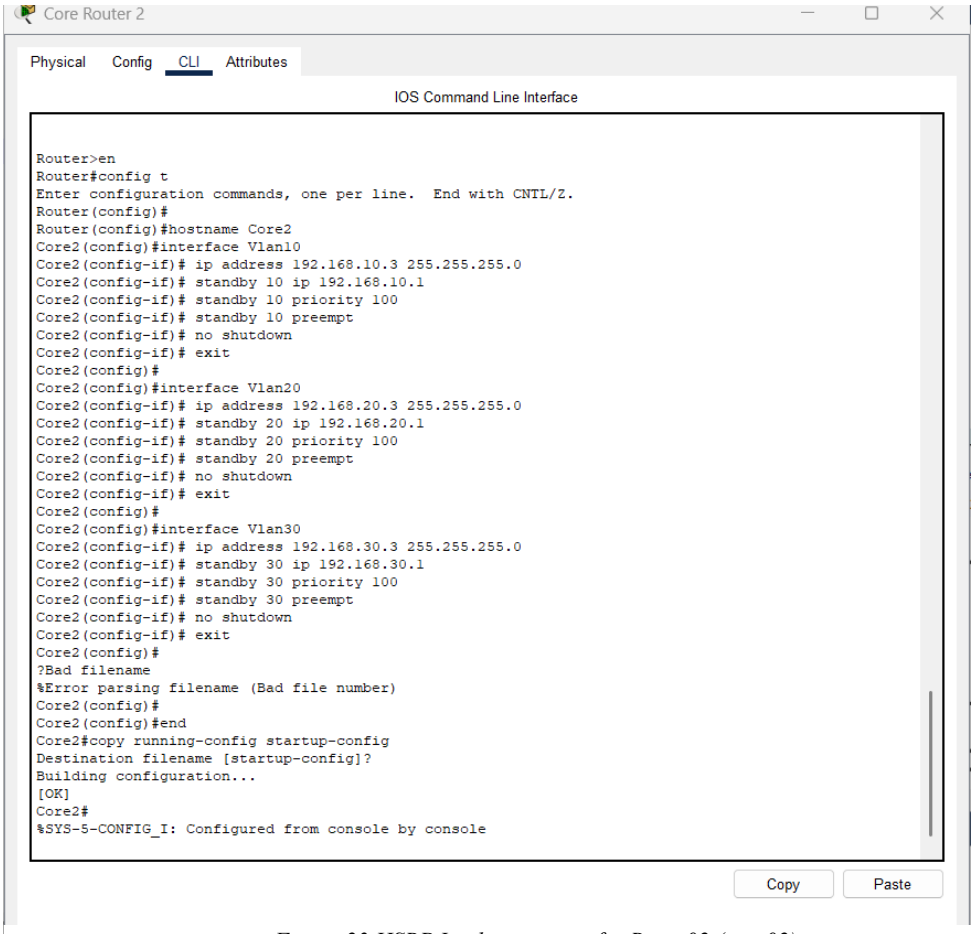

Figure 23 HSRP Implementation for Route02 (core02)

3.6.1 After Apply HSRP Implementation

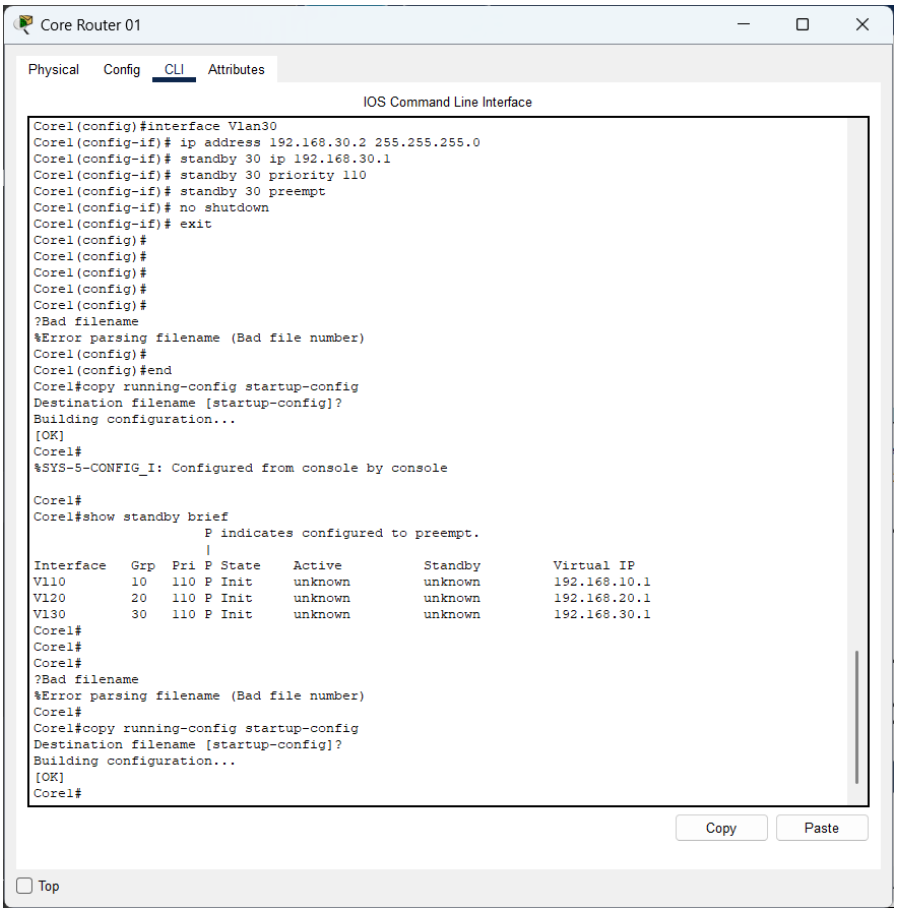

Figure 24 After apply HSRF Implementation Check Status in Router 01

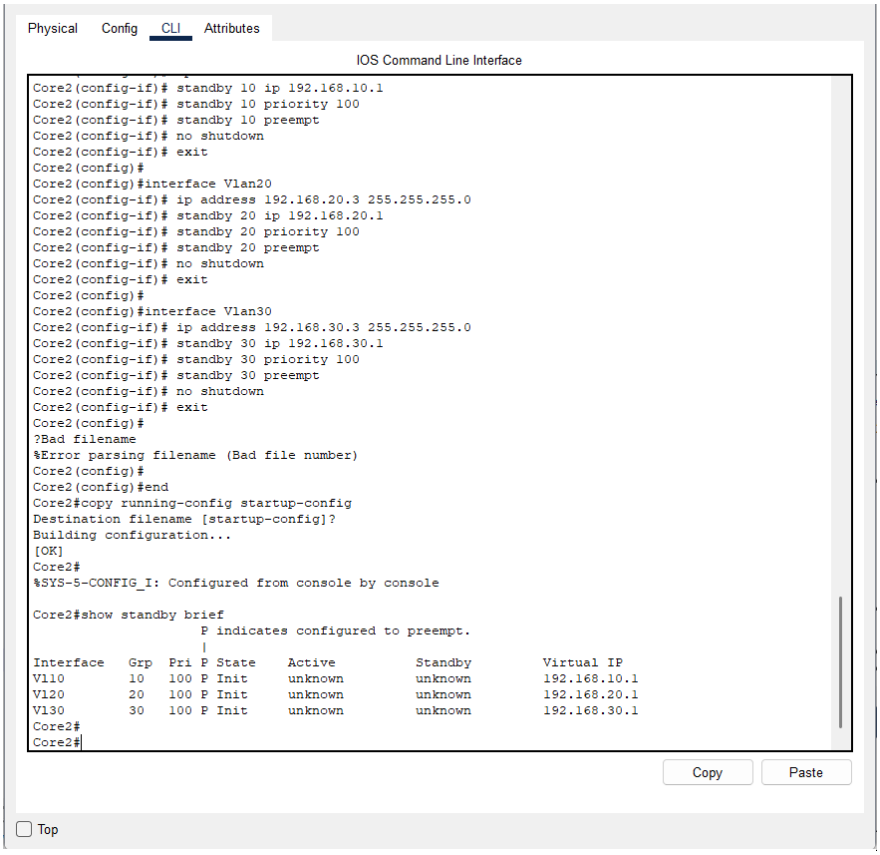

Figure 25 After apply HSRF Implementation Check Status in Router 02

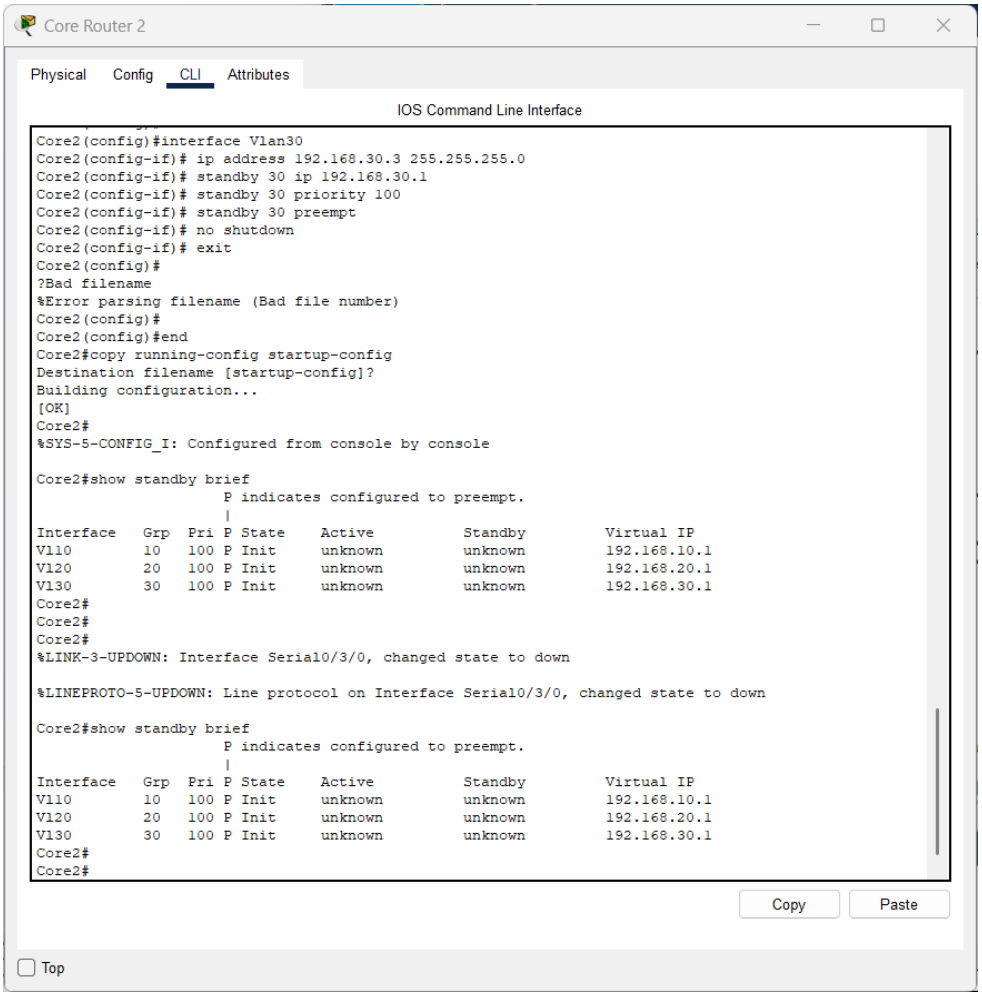

Figure 26 After apply When power of Router 01Check Status in Router 02

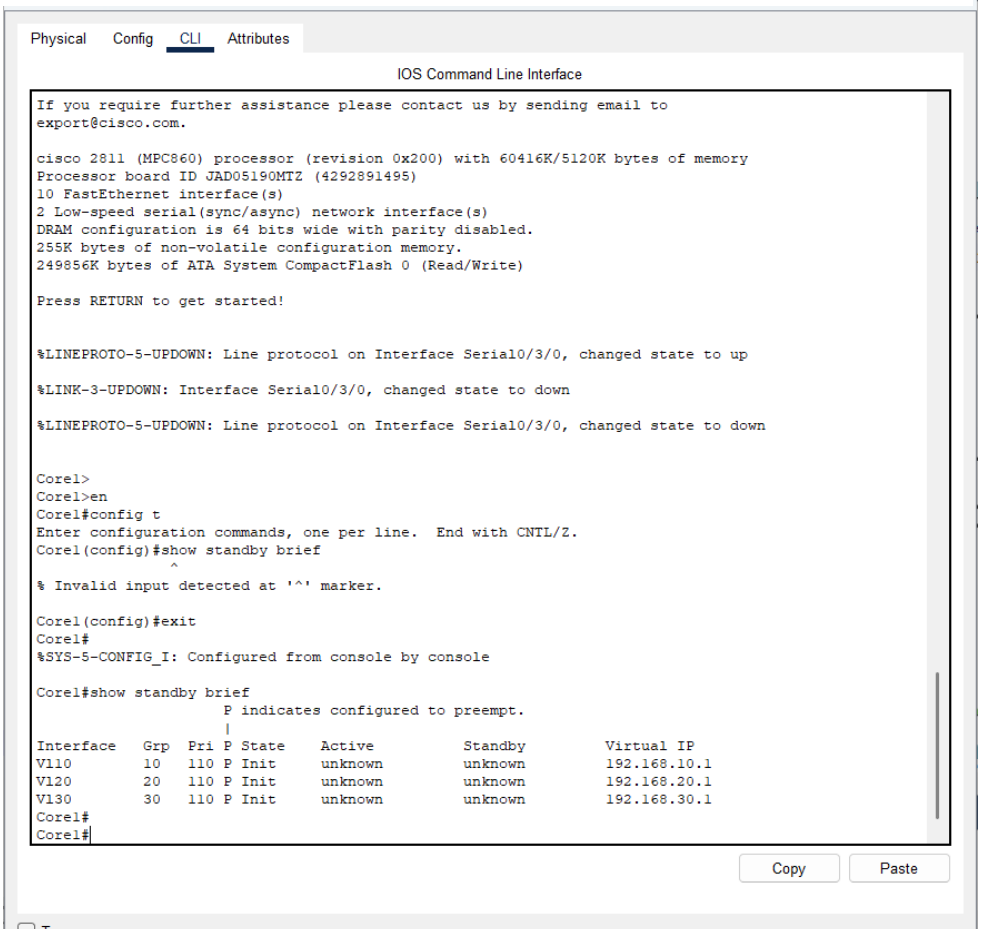

Figure 27 After apply When power of Router 02 Check Status in Router 01

References

- Contributor, T. (2023, June 20). *TechTarget Network* . Retrieved from https://www.techtarget.com/searchstorage/definition/failover

- Dooley, K. (2024, June 03). *Network Redundancy and Why It Matters*. Retrieved from Auvik.com: https://www.auvik.com/franklyit/blog/simple-network-redundancy/

- *HSRP (Hot Standby Routing Protocol)*. (n.d.). Retrieved from NetworkLessons: https://networklessons.com/cisco/ccie-routing-switching/hsrp-hot-standby-routing-protocol

- Kareemoddin, M. (2016, November 05). *Network & Security Consultant* . Retrieved from HSRP State: https://www.kareemccie.com/2016/11/hsrp-states.html

- *Understand the Hot Standby Router Protocol Features and Functionality*. (2023, September 13). Retrieved from Cisco: https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html