CAREER EPISODE:2

INTRODUCTION:

CE 2.1 During my [redacted] at [redacted] Australia, I worked on the assessment tasks on "Plan and Manage troubleshooting advanced integrated IP networks (ICTNWK612)", in [redacted] I designed, configured, tested, monitored and troubleshot an enterprise style network infrastructure using switching, routing, VLANs and network management tools.

BACKGROUND:

CE 2.2 As part of my diploma studies, I worked on Plan and Manage troubleshooting advanced integrated IP networks assessment where I built and managed a simulated organizational network environment. I implemented VLAN segmentation, PVLANs, SVIs and IPv4/v6 addressing to enhance communication, security and network efficiency. I performed network testing using; ping, traceroute, Wireshark, SNMP and Syslog to monitor performance and identify faults. I developed router maintenance procedures, monitored IOS configuration and routing behavior. I analyzed network operations across various OSI layers to isolate problems related to MAC addresses, ARP tables and IP addressing. I tested switch to switch connectivity, trunk links, access ports, loop prevention via STP and advanced switch services like BERT, RFC 2544 performance testing and misconfigurations, trunking problems, IP conflicts, subnetting errors and native VLAN mismatches, that helped me gain practical experience in network configuration, troubleshooting, monitoring and infrastructure optimization.

REPORTING HIERARCHY:

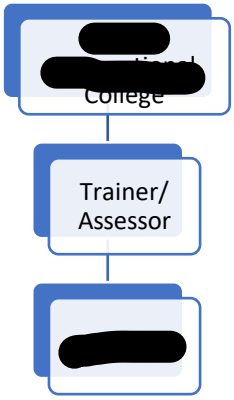


Figure 1: Hierarchy

PERSONAL ENGINEERING ACTIVITIES:

Network Routing, Router Operations & VLAN Implementation:

CE 2.3 During my diploma I was given an assessment task where I worked on the configuration, verification and troubleshooting of routing and VLAN based network systems to understand and implement core networking concepts in practical environments. I configured routing using static, dynamic and default routes for communication between various networks. I used routing protocols like routing information protocols, open shortest path first and border gateway protocol for efficient path selection and adaptability in network topology. I configured routers by assigning IP addresses, enabling interfaces, securing access and checking operation using routing tables and interface status commands. In troubleshooting, I identified and overcame problems by checking physical connectivity, interface configurations, routing entries and protocol neighbor relationships for proper network functionality. I also implemented VLANs to segment network logically for enhanced performance and security, configuring access and trunk ports using IEEE 802.1Q protocol and inter VLAN communication via layer3 routing methods. It helped me develop strong practical understanding of routing, switching and network troubleshooting.

IP Networking Concepts, Systems & Infrastructure Design:

CE 2.4 I understood and applied main IP networking concepts; WSNs, OSI/TCP-IP models, IOS systems, network topologies and core IP infrastructure elements as part of my task. I reviewed WSN deployment schemes like random, grid based, deterministic, cluster based and mobile deployment. I learned how they affect coverage, energy efficiency and data reliability in real-world monitoring systems. I explored IP networking models; OSI model and TCP/IP model. I learned how every layer handles communication from physical transmission to application level services. I worked on Cisco IOS and Cisco internetwork operating system, where I studied CLI based configuration, routing, switching, security and monitoring services. I also analyzed IP network topologies like star and mesh structures to assess scalability, redundancy and fault tolerance in network design. I learned about IP network architecture; access, distribution and core layers. I applied knowledge of fundamental network components like IP addressing, routers, switches and firewalls to design and understand communication systems. It helped me develop practical knowledge of telecom network planning, infrastructure design and troubleshooting, as per the real-world engineering and service provider network operations.

Network Testing, Monitoring, Standards, Protocol & VLAN Implementation:

CE 2.5 I understood and applied main concepts of network testing, monitoring, standards, protocols, threat mitigation and VLAN technologies. I performed network testing to assess performance, reliability and security by analyzing bandwidth, latency, packet loss, connectivity and system vulnerabilities for optimal network working and compliance with service requirements. I applied testing in various scenarios; performance security, connectivity, load and compliance testing to identify bottlenecks, check system capacity, secure communication and confirm adherence to standards. I used protocols; SNMP, ICMP, NetFlow, and Syslog to monitor traffic, detect faults and manage device performance in real time. I worked with monitoring tools; Cisco Meraki and SolarWinds network performance monitor to notice bandwidth usage, latency, device health and security events using centralized dashboards and automated alerts. I also explored network standards like IEEE 802.3 Ethernet, IEEE 802.11 Wi-Fi and TCP/IP to understand interoperability, scalability and communication reliability between various systems. I analyzed network protocols; TCP, UDP, SSL/TLs, IPsec, OSPF and BGP for communication, security, routing and management functions. I implemented my understanding of VLAN technologies by segmenting networks logically using IEEE 802.1Q and configuring inter VLAN routing to enhance performance, security and scalability. It helped me develop strong understanding of system monitoring, troubleshooting and secure infrastructure design as per the industry engineering standards.

CE 2.6 I planned, managed, tested and troubleshot complex IP based enterprise networks in a simulated environment. I developed strategies to monitor and optimize IP network performance by analyzing traffic flow, bandwidth utilization, latency, packet loss, device network monitoring dashboards. I noticed critical network devices; routers, switches, firewalls, servers and access points. I confirmed continuous monitoring via data sources; flow data, packet captures, Wi-Fi metrics and SNMP based device data. I implemented network segmentation and troubleshooting isolation strategies using VLANs, access control and least privilege principles to separate network segments for efficient fault detection. I designed and executed testing scenarios covering server client communication, data migration, cloud infrastructure validation, network level performance, installation, deployment checks and test environment simulations for system reliability and scalability. I tested VLAN based solutions; switch to switch connectivity, access ports, loop prevention, PVLANs and switch virtual interfaces for correct inter switch communication. I also produced a maintenance plan for monitoring routing protocols and configurations using tools and

commands related to Cisco IOS, checking for stability for routing functions in both IPv4 and v6. I applied OSI layer-based troubleshooting to isolate faults; duplicate IP addresses, DNS problems, slow performance, VLAN trunking errors and interface features. I developed security monitoring techniques for IOS services by adding intrusion detection, firewall policies and log analysis for mission critical apps. It helped in reliable network operations, enhanced fault resolution efficiency and maintained optimal performance.

Testing, Monitoring Tools Selection & IOS Maintenance for IP Network Troubleshooting & Performance Management:

CE 2.7 I chose, implemented and managed appropriate network testing and monitoring tools for troubleshooting and performance optimization. I used network testing tools; ping, traceroute, Wireshark, NetFlow analyzers, iperf and Nmap to diagnose connectivity problems, measure latency, analyze bandwidth usage and identify security vulnerabilities across the IP network. For continuous monitoring, I applied Nagios, SolarWinds network performance, PRTG network monitor, Zabbix and ManageEngine OpManager to track device health, network performance, traffic flow and system alerts in real time. I configured dashboards, automated alerts and reporting mechanisms for proactive detection of faults and performance degradation. I also implemented monitoring strategies using SNMP, Syslog and ICMP protocols to collect performance data, centralize logs and check device availability across the network. I also developed and followed IOS maintenance plan where I checked router configuration, monitored routing protocols like OSPF, RIP and EIGRP and checked that firmware updates and backups are performed securely. I checked IOS memory architecture, managed its upgrades and ensured correct boot configurations for system stability. I monitored routing tables, interface status and configuration integrity using show commands and backup comparisons to detect unauthorized changes/faults.

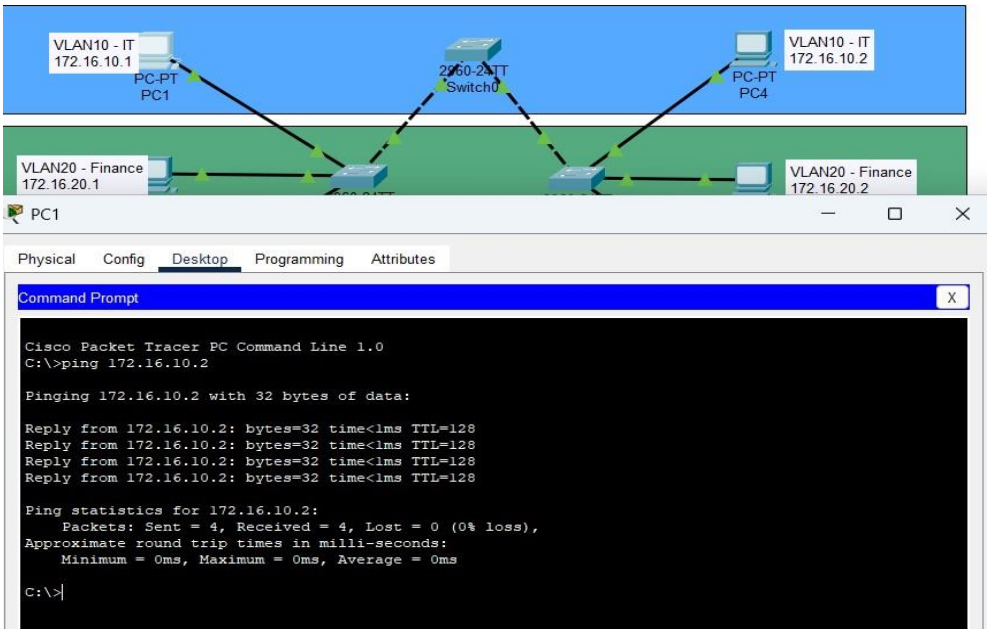


Figure 2: Connectivity verification using ping between PC1-4 in VLAN10

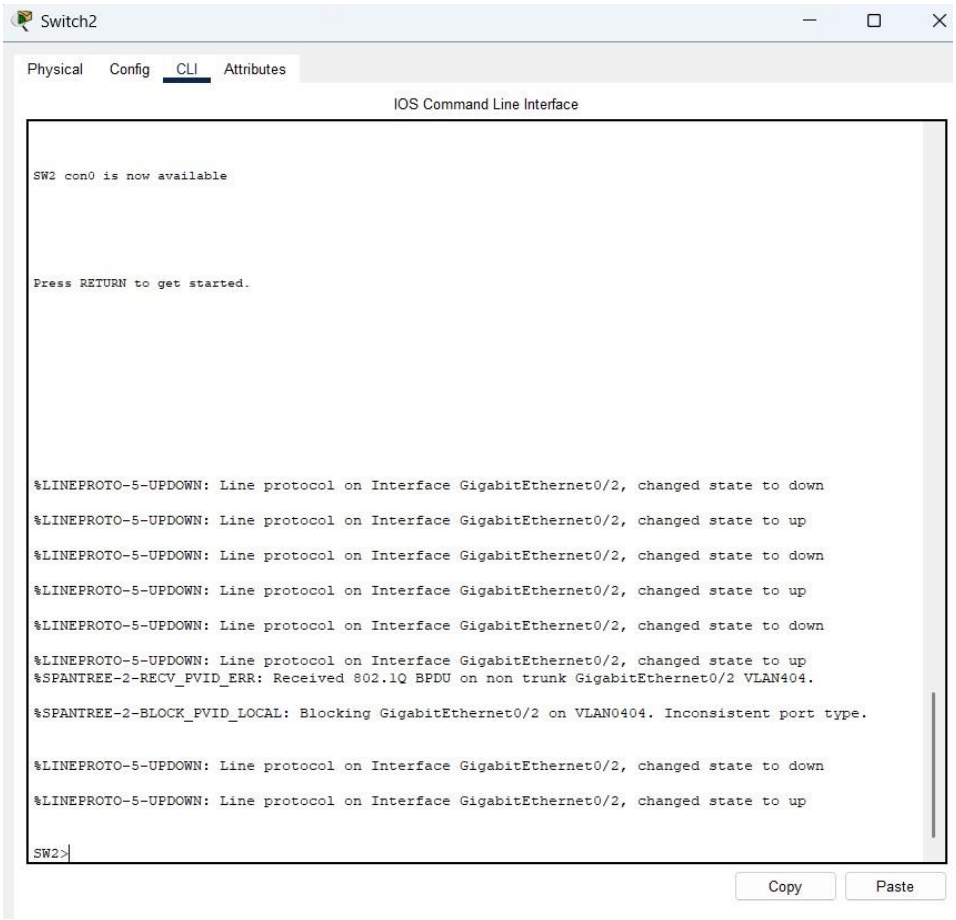


Figure 3: Network monitoring using SNMP and centralized Syslog analysis

OSI Based Network Fault Isolation & IOS Security Troubleshooting Plan:

CE 2.8 I used Open system Interconnection model to isolate suboptimal internetwork operations and enhance the performance and reliability of the training organizations' integrated IP

network. I applied layer by layer troubleshooting technique to identify faults systematically. At the physical layer, I checked cables, ports, interface status, speed and duplex adjustments to detect connectivity problems. At the data link layer, I analyzed VLAN configuration, trunk links, MAC address tables and ARP mappings to identify broadcast storms, VLAN trunking problems, MAC conflicts and incorrect layer2 addressing. At the network layer, I reviewed IP addressing, subnet allocation, routing cables and gateway configurations to overcome duplicate IP addresses, IP exhaustion and routing inefficiencies. I also checked transport layer communication using TCP and UDP sessions. At the Application layer, I checked DNS services and app availability for service continuity. Using this, I isolated faults more efficiently and enhanced network stability.

CE 2.9 For troubleshooting and monitoring Cisco IOS services mission critical apps, I used various IOS diagnostic tools and monitoring methods. I used show commands; show version, show running-config, show interfaces and show ip route to monitor router health, interface performance and routing protocol behavior. I used debug commands to analyze protocol specific problems and isolate configuration issues, while checking that the processor resources were protected by disabling debugging after use. I used the ping command to check connectivity, latency and packet loss between devices and network segments. For physical media troubleshooting, I used TDRs and OTDRs to detect cable faults in copper and fiber links. I also applied BERTs/ BLERTs and breakout boxes to test digital interface signals and identify communication errors. I also used network monitors and protocol analyzers to capture traffic, establish performance baselines, analyze packet flows and detect anomalies. This troubleshooting and monitoring approach helped me maintain secure, reliable and optimized IOS based network functions.

IPv4/IPv6 Interoperability Planning & VLAN Connectivity Testing:

CE 2.10 I developed a plan for troubleshooting and monitoring interoperability between IPv4 and v6 for reliable communication, scalability and future readiness of the network. I started by preparing an addressing table by assigning IPv4 addresses to end devices across multiple VLANs and planned IPv6 addressing to support dual stack implementation. I configured VLAN 10, 20 and 30 with separate subnet allocations for segmentation and enhanced traffic management. I then evaluated network operations by performing connectivity tests like ping and traceroute between devices to check end to end communication and routing functionality. I checked VLAN trunking, access port assignments, inter VLAN routing and default gateway configuration for proper packet forwarding across both IPv4 and v6. I used simulation tools to analyze packet movement through various OSI layers and identify

addressing/routing problems. After collecting data through device logs, SNMP polling and packet captures, I created an action plan to isolate faults, correct IP conflicts, optimize subnetting and enhance routing performance. This process enhanced my skills in internetwork planning, IP addressing strategy and protocol interoperability.

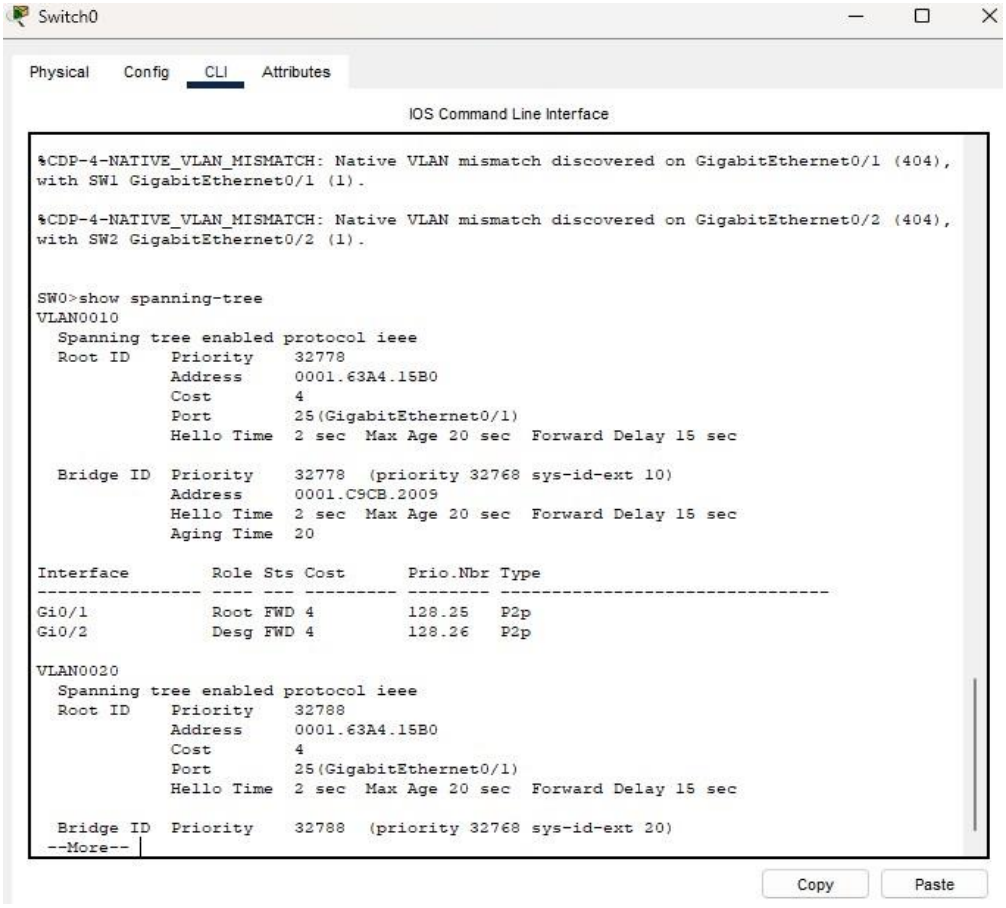


Figure 4: Loop prevention in VLAN based network using STP

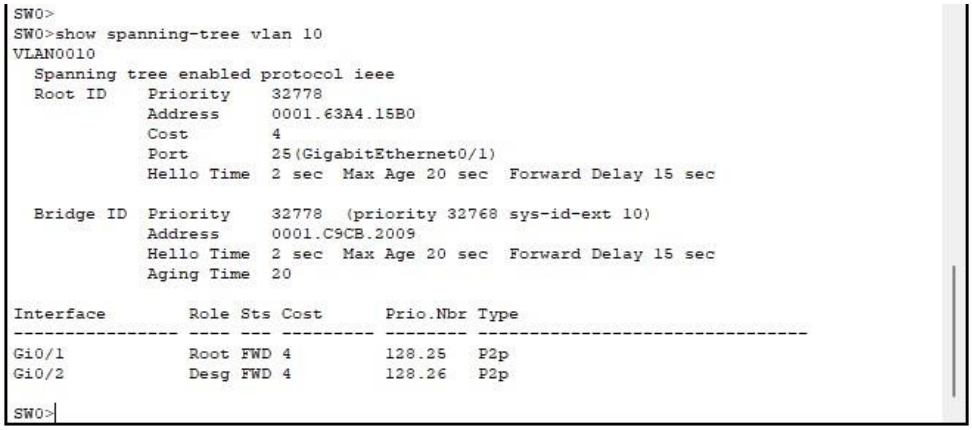


Figure 5: Switch0 Spanning-tree VLAN10

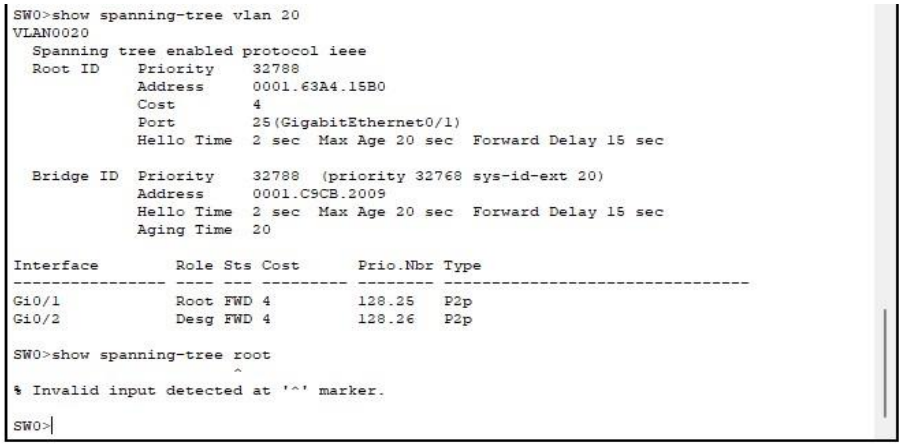


Figure 6: Switch0 Spanning-tree VLAN20

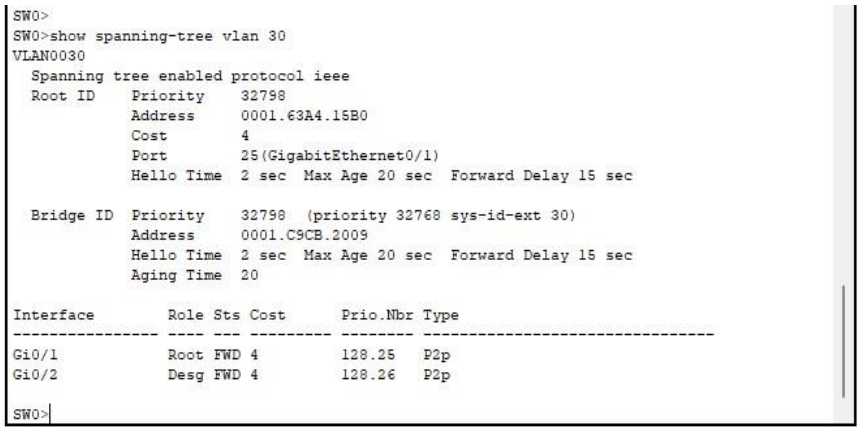


Figure 7: Switch0 Spanning-tree VLAN30

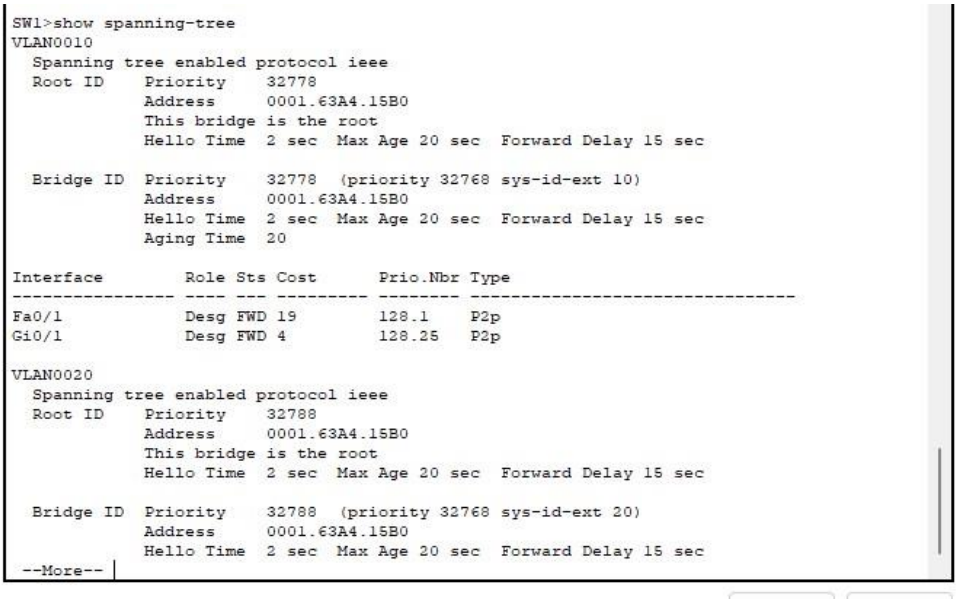


Figure 8: STP interface status & blocked link verification on switch1

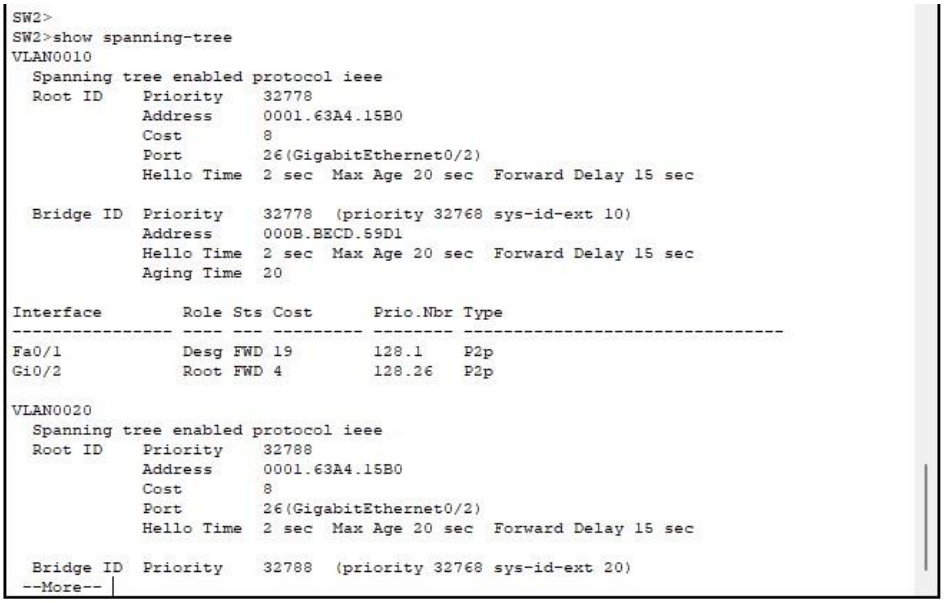


Figure 9: STP interface status & blocked link verification on switch2

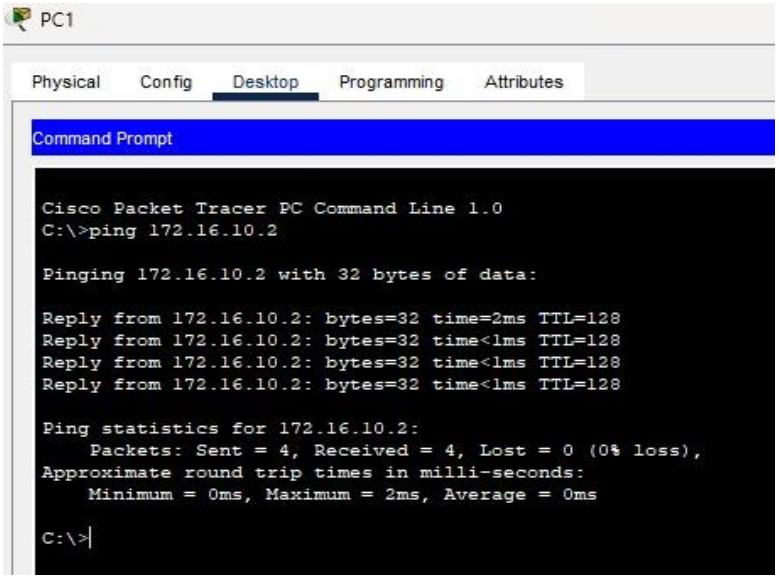


Figure 10: Inter VLAN connectivity verification using ping test between VLAN devices

VLAN Validation, SVI Testing, Advanced Switch Service Verification & Configuration Troubleshooting:

CE 2.11 I tested PVLANs, SVIs, advanced switch services and performed complete switch troubleshooting to enhance network segmentation, reliability and security. I connected the VLAN environment and validated PVLAN implementation to control layer2 communication between devices. I checked the primary VLAN and related PVLAN mappings for isolated, community and promiscuous port communication to behave as per design requirements. Using packet analyzer and simulation model, I captured and checked incoming traffic to validate VLAN tagging and traffic isolation for VLAN 10, 20 and 30. Through packet level

inspection, I checked that every VLAN maintained proper segmentation and that unauthorized inter VLAN communication was blocked. I then tested SVIs by checking that the required VLANs existed in the VLAN database before assigning layer3 interfaces for inter VLAN routing. I used the autostate mechanism for SVI to remain operational by checking that at least one active access port existed in VLAN. I also checked trunk configurations for all SVI VLANs to be allowed across inter switch links, full inter VLAN communication. These tasks enhanced my knowledge of VLAN architecture, layer2 security design and layer3 switching operations.

CE 2.12 I checked advanced switch services by conducting BERT, RFC 2544 performance testing and multi stream traffic testing to assess switch performance under operational loads. During BERT testing, I checked abnormal bit errors on backbone trunk link and isolated the problem to a faulty UTP cable, that I changed to restore signal integrity. Through RFC 2544 testing, I analyzed throughput, latency and frame loss between core and access switches, where I identified trunk VLAN misconfiguration affecting VLAN20 and corrected the allowed VLAN list to restore normal performance. In multi stream testing, I simulated traffic from several VLANs to assess QoS, bandwidth allocation and switch stability under load and overcame VLAN trunk mismatches affecting VLAN30 traffic. I then troubleshot switch configuration problems by defining the issue, collecting data, checking ARP cache entries, MAC address tables and peripheral switch learning behavior. I identified duplicate IP addressing, subnet mask mismatches, VLAN assignment errors, trunk misconfigurations and native VLAN mismatches and corrected them using Cisco CLI commands; show vlan brief, show interfaces trunk and show mac-address-table. After implementing corrections, I verified communication between devices in the same VLAN while maintaining isolation between separate VLANs. It showed my ability to troubleshoot, switch optimization, default isolation and infrastructure planning.

```
SW0>show vlan

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
10   IT                               active
20   Finance                          active
30   HR                               active
404  Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
 --More--
```

Figure 11: Primary VLAN and PVLAN

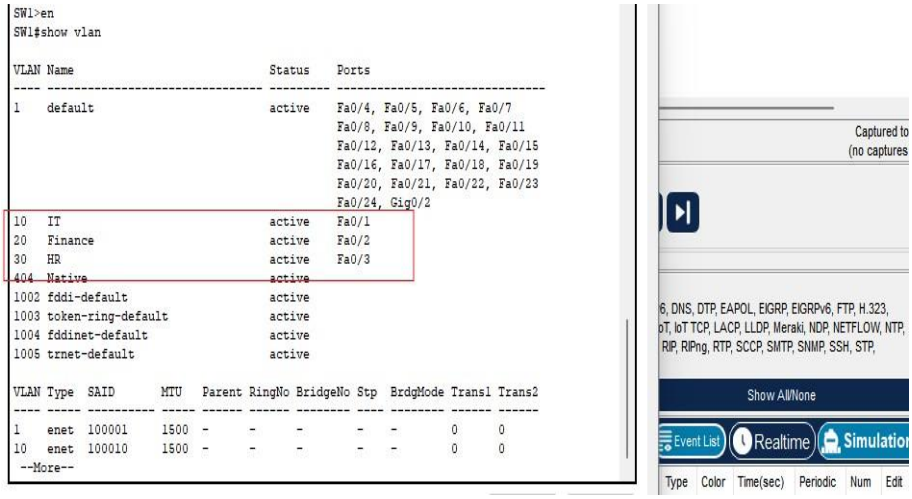


Figure 12: VLANs status & ports

Figure 13: Ping test

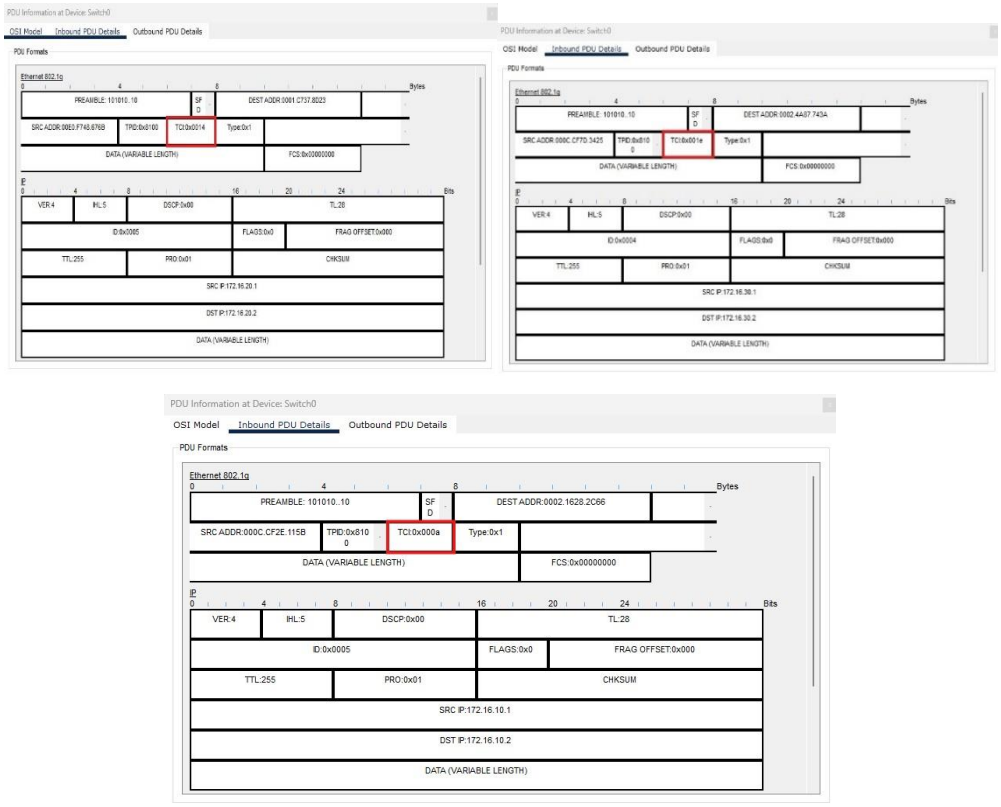


Figure 14: Packet capture verification of VLAN10

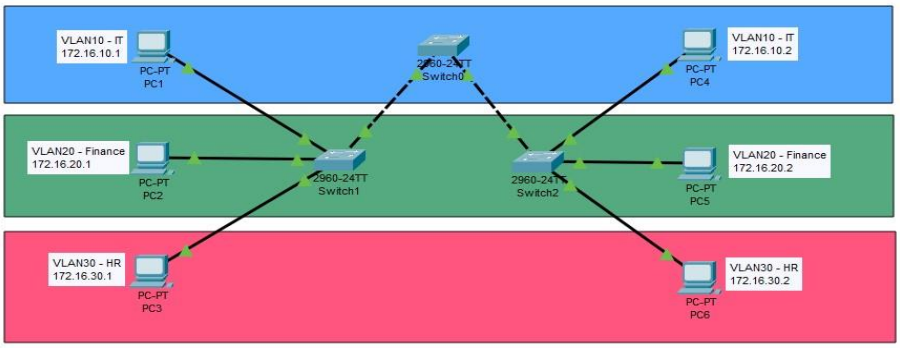


Figure 15: Network topology

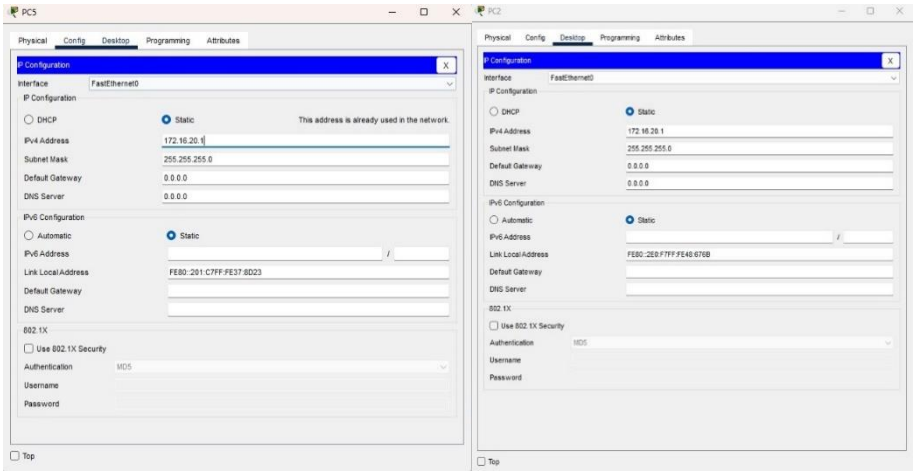


Figure 16: ARP cache analysis and duplicate IP address issue between PC1- 5

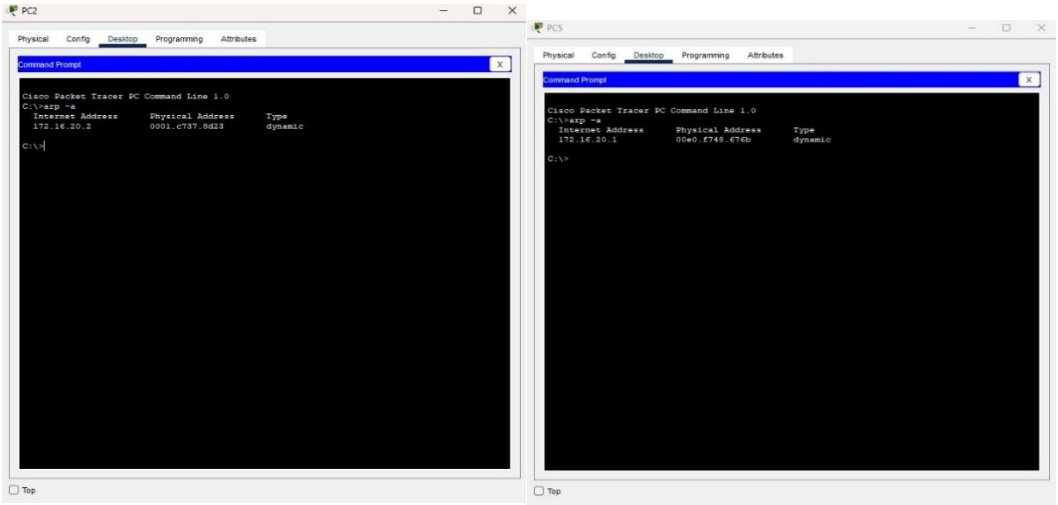


Figure 17: Resolution of network disruption by correcting IP address assignment

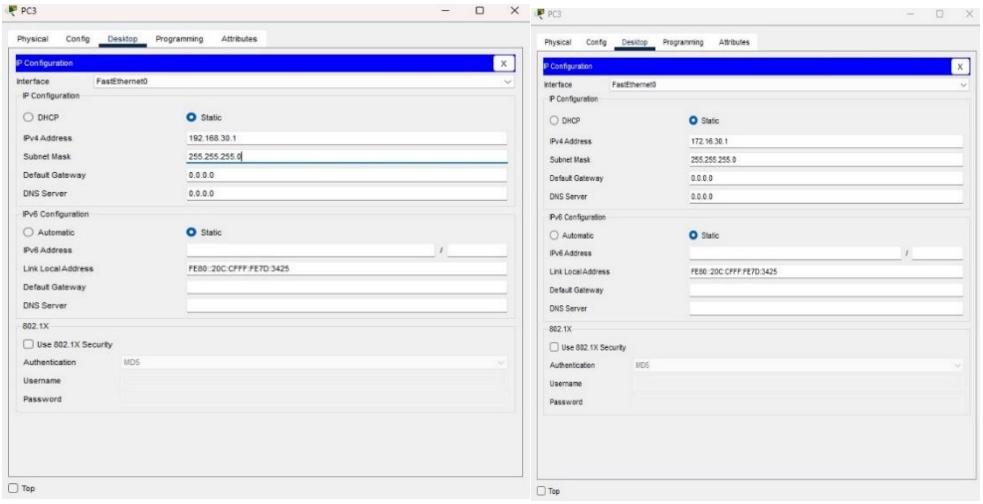


Figure 18: Correction of IP misconfiguration on PC3 restoring VLAN30 connectivity

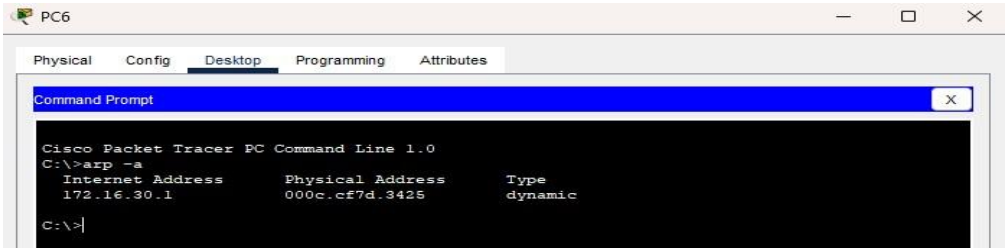
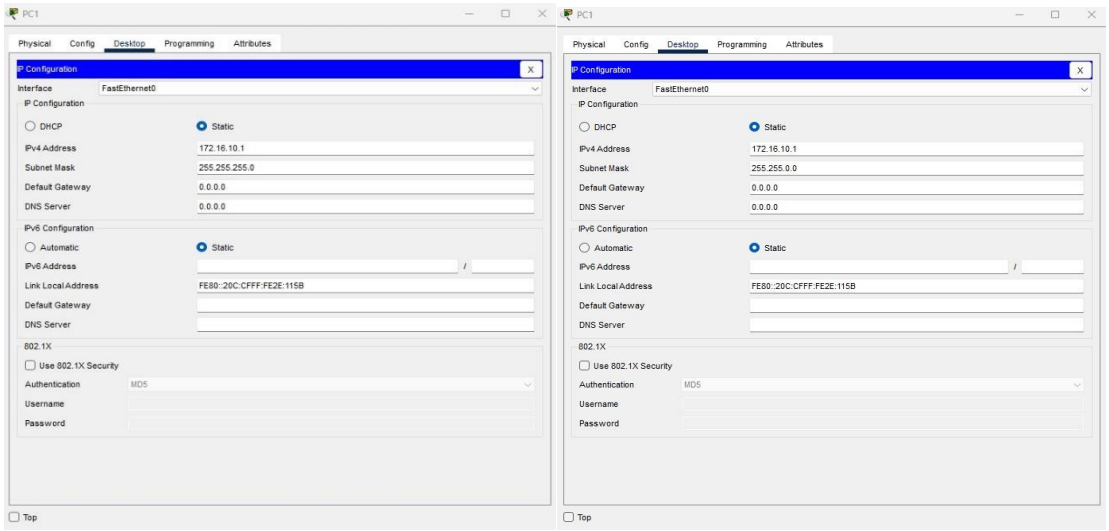


Figure 19: PC6 ARP cache showing correct IP address of PC3



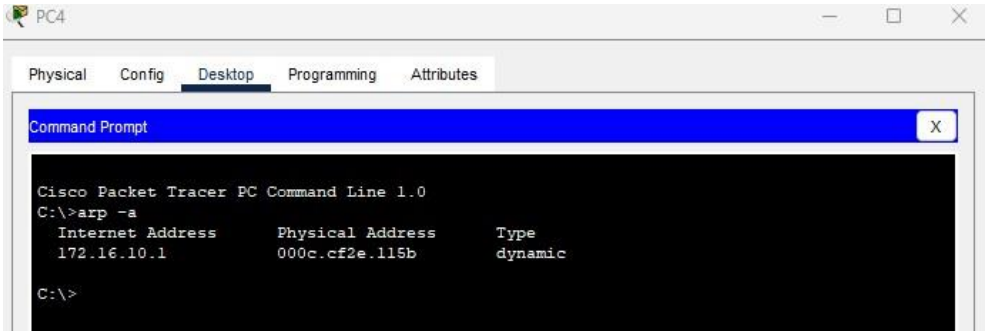


Figure 20: Correction of incorrect subnet mask on PC1 and security risk mitigation VLAN10

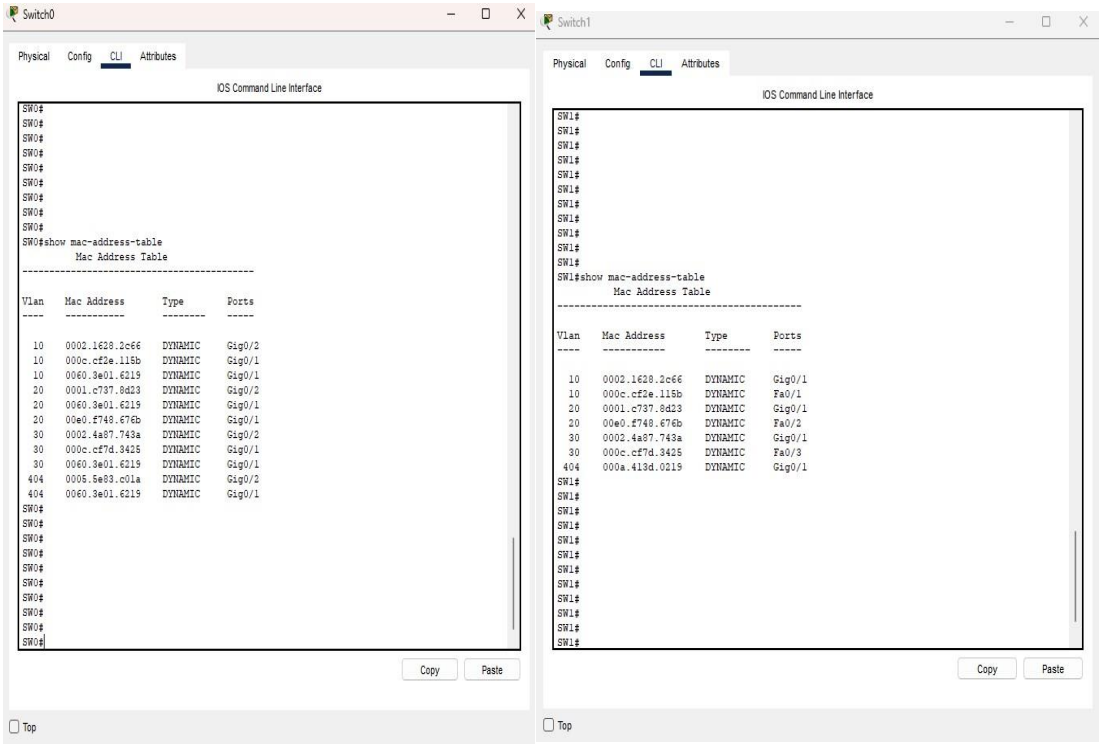


Figure 21: MAC address table verification across all switches

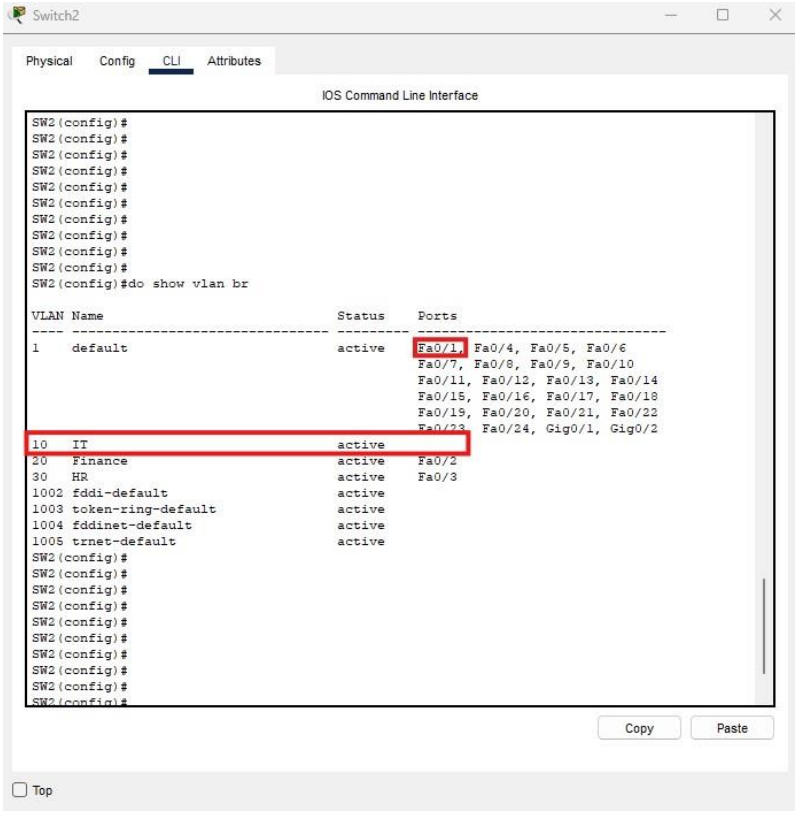


Figure 22: PC4 not assigned to VLAN10 access port on switch2

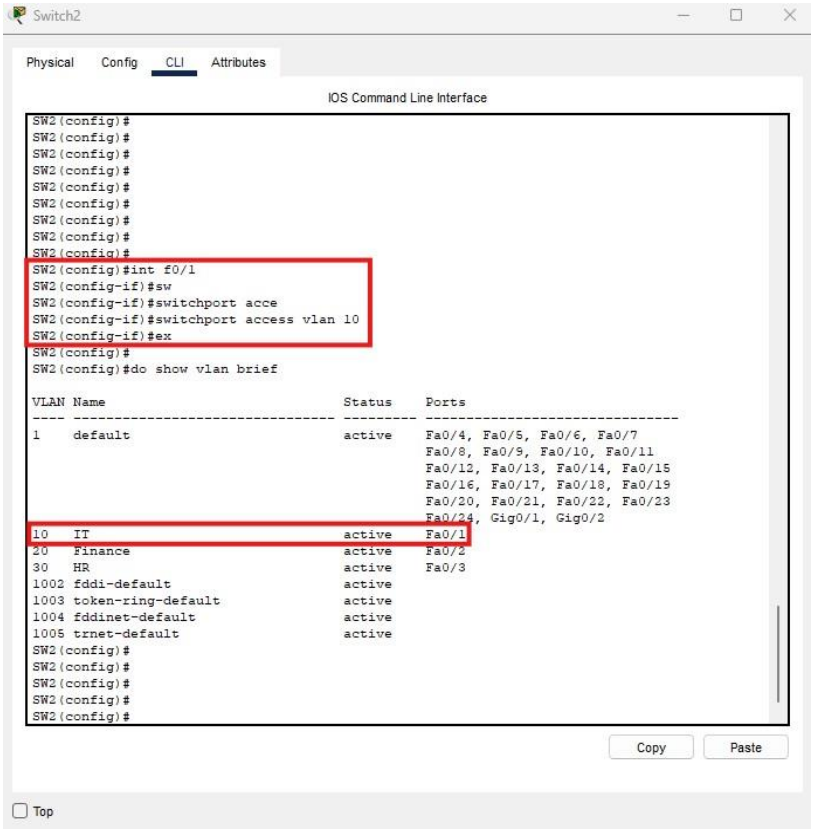


Figure 23: Assignment of PC4 to VLAN10 on switch2

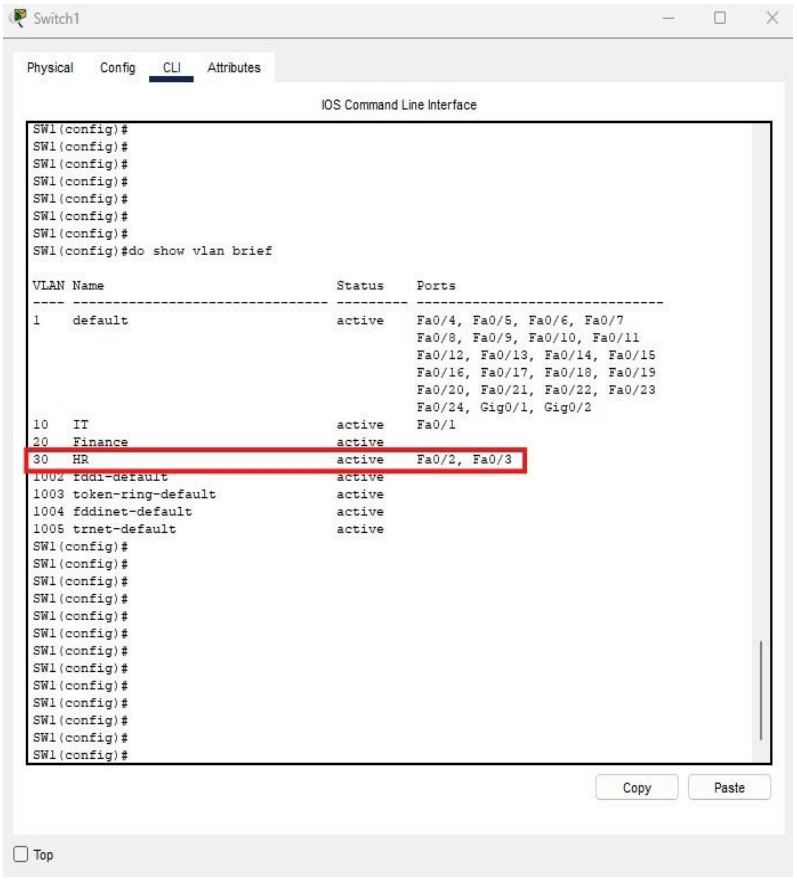


Figure 24: VLAN30 misconfiguration on switch1

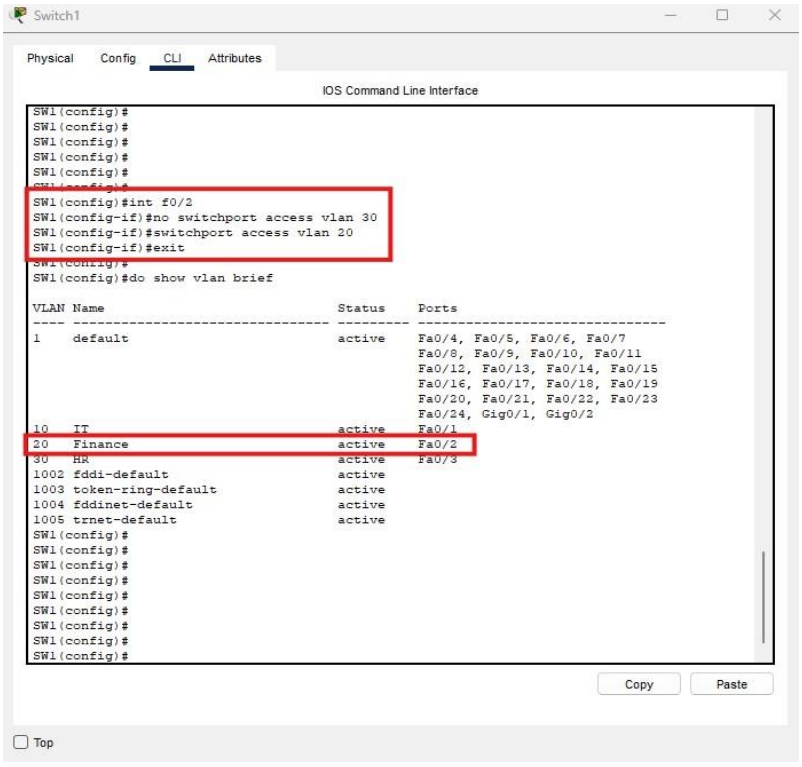


Figure 25: Reassignment of PC2 from VLAN 30-20 on Fast Ethernet 0/2

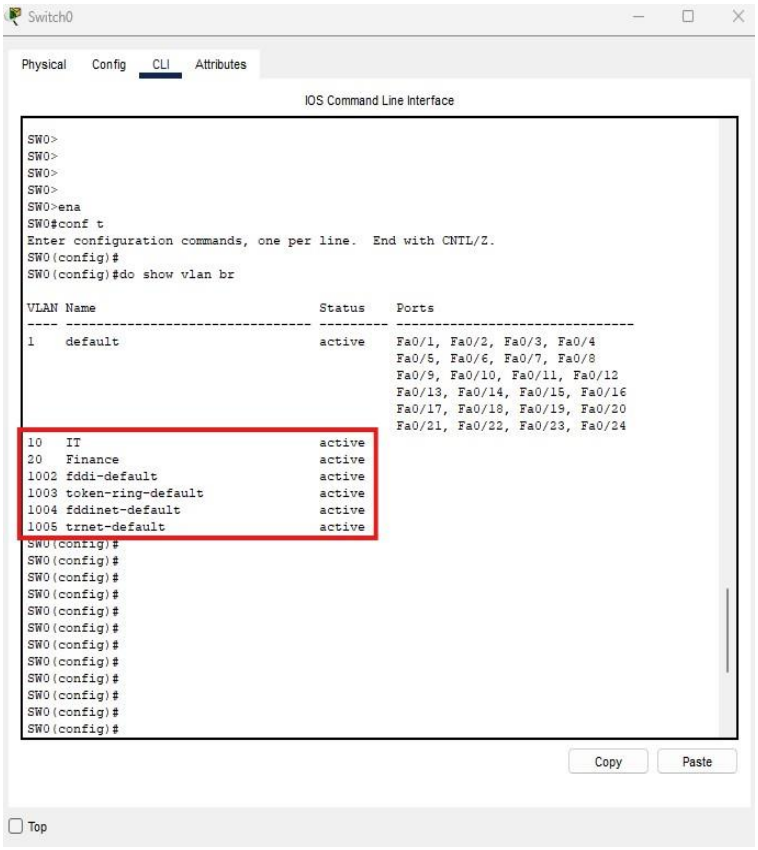


Figure 26: Missing VLAN30 on switch-0 causing backbone communication failure

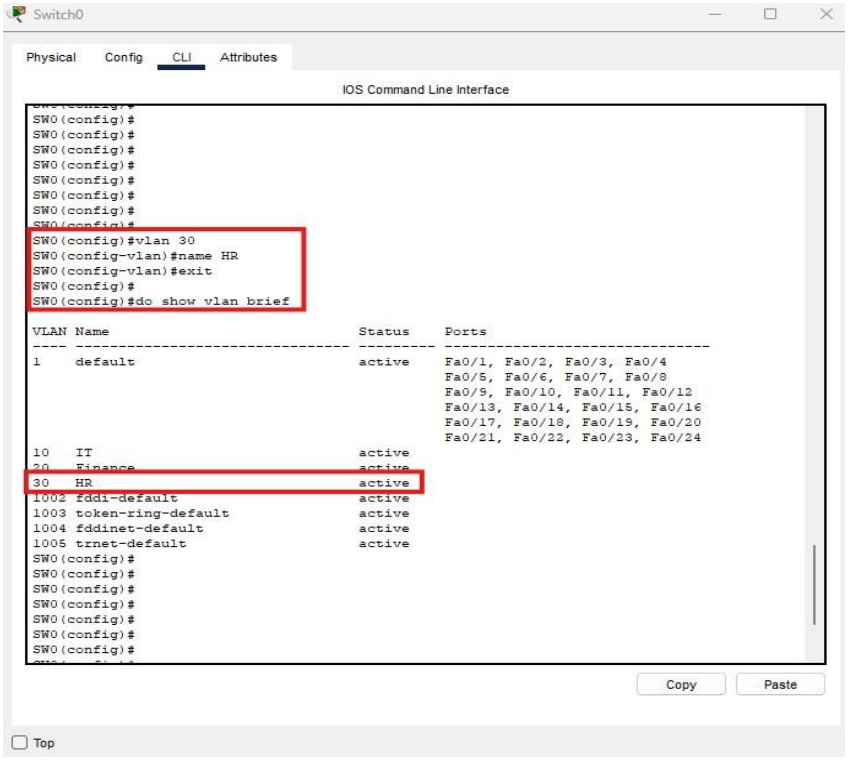


Figure 27: VLAN30 creation and naming as HR on switch-0

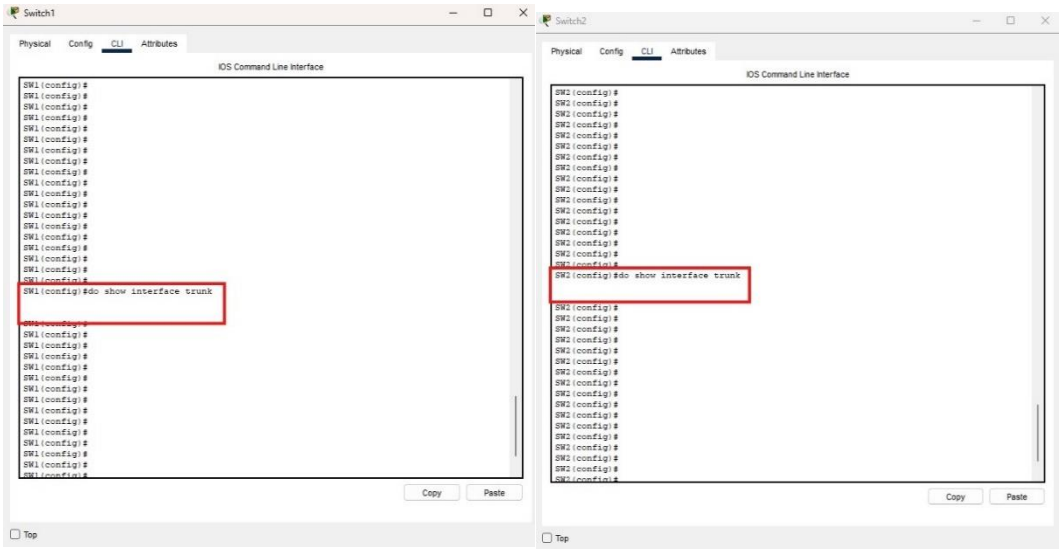


Figure 28: Trunk configuration problem on switch1-2 Gigabit ports

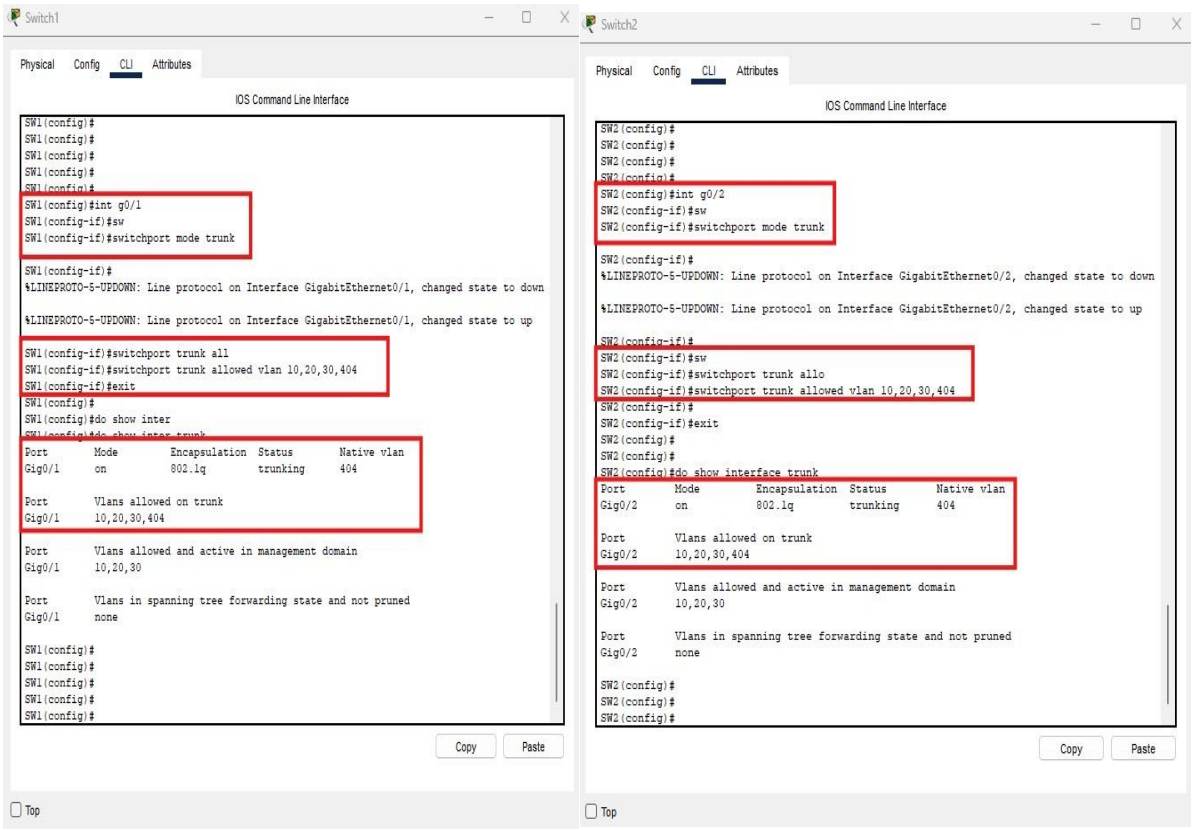


Figure 29: Trunk configuration on switch1-2 with VLANs

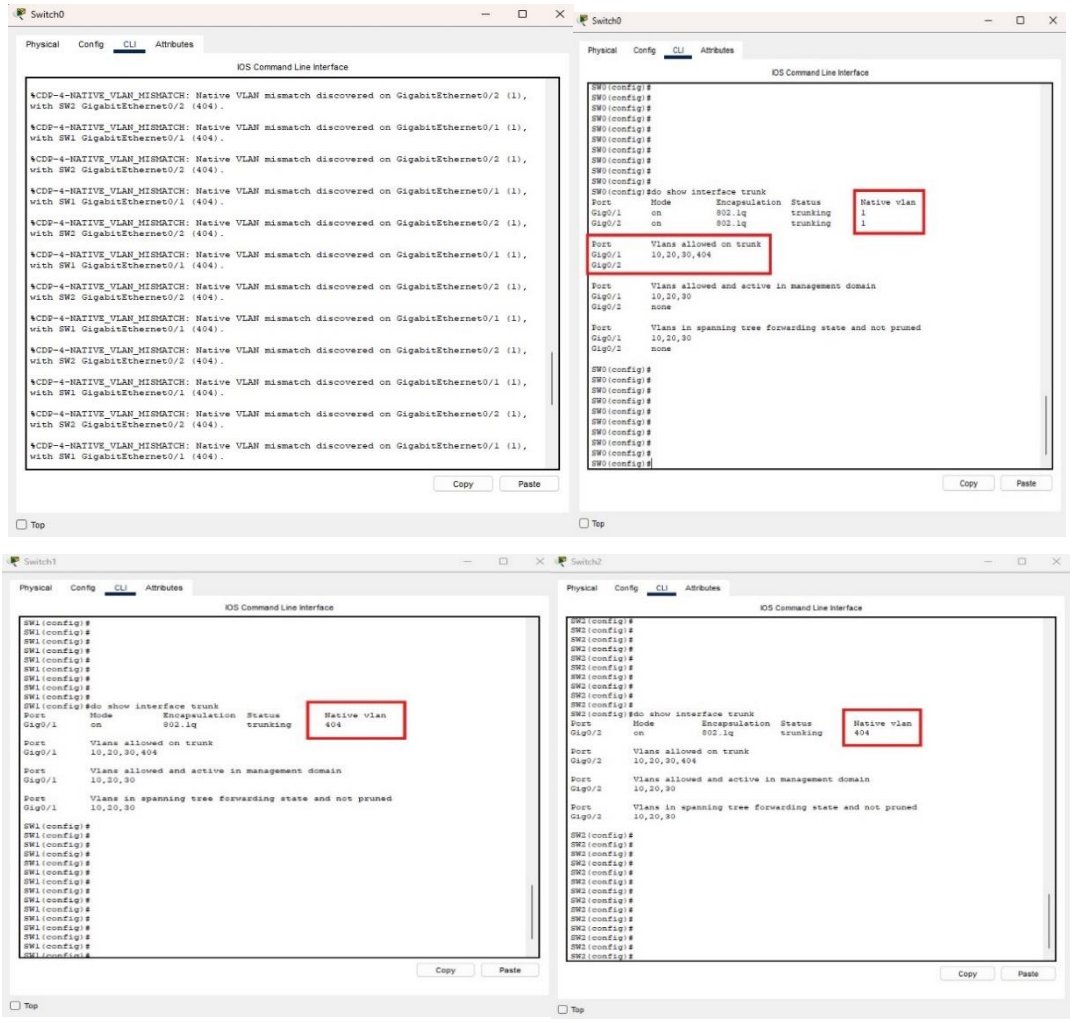


Figure 30: native VLAN mismatch and missing allowed VLANs on switch0-2 links

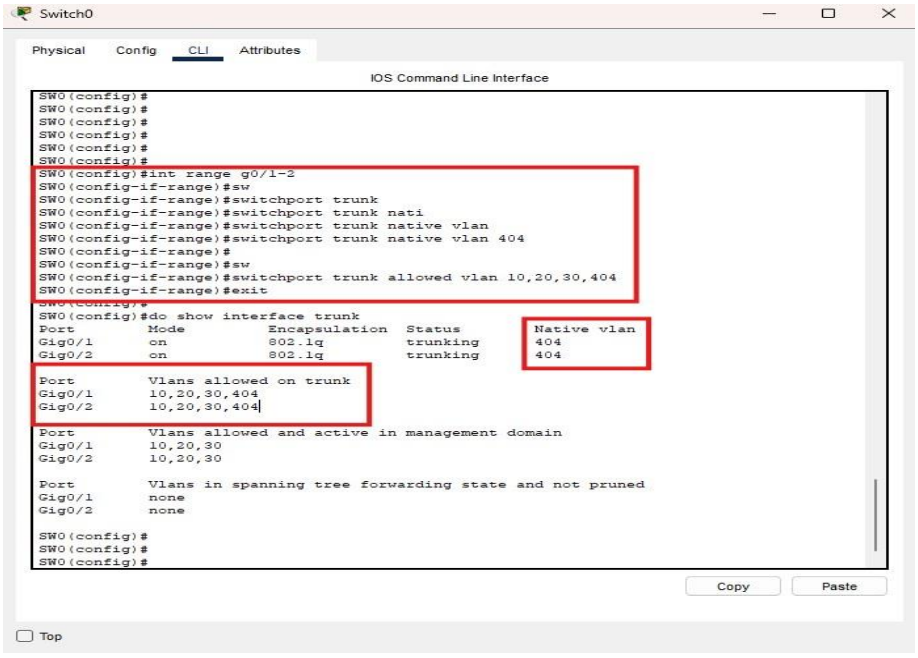
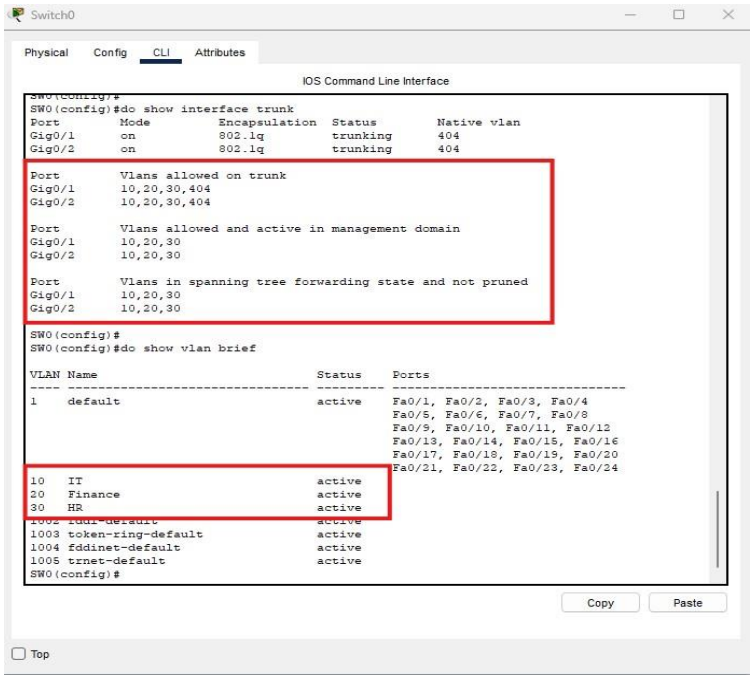
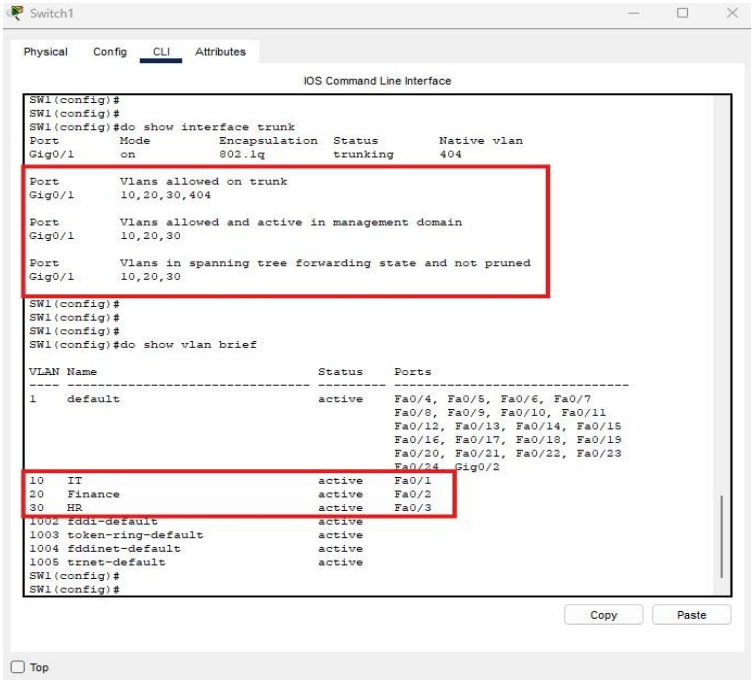


Figure 31: Native VLAN change to 404 and allowed VLANs on trunk 10, 20 30, 404


Switch0
Physical
Config
CLI
Attributes
IOS Command Line Interface
SW0(config)#do show interface trunk
Port Mode Encapsulation Status Native vlan
Gig0/1 on 802.1q trunking 404
Gig0/2 on 802.1q trunking 404
Port Vlans allowed on trunk
Gig0/1 10,20,30,404
Gig0/2 10,20,30,404
Port Vlans allowed and active in management domain
Gig0/1 10,20,30
Gig0/2 10,20,30
Port Vlans in spanning tree forwarding state and not pruned
Gig0/1 10,20,30
Gig0/2 10,20,30
SW0(config)#
SW0(config)#do 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
10 IT active
20 Finance active
30 HR active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
SW0(config)#
Copy
Paste
Top


Switch1
Physical
Config
CLI
Attributes
IOS Command Line Interface
SW1(config)#
SW1(config)#
SW1(config)#do show interface trunk
Port Mode Encapsulation Status Native vlan
Gig0/1 on 802.1q trunking 404
Port Vlans allowed on trunk
Gig0/1 10,20,30,404
Port Vlans allowed and active in management domain
Gig0/1 10,20,30
Port Vlans in spanning tree forwarding state and not pruned
Gig0/1 10,20,30
SW1(config)#
SW1(config)#
SW1(config)#
SW1(config)#do 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, Gig0/2
10 IT active Fa0/1
20 Finance active Fa0/2
30 HR active Fa0/3
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
SW1(config)#
SW1(config)#
Copy
Paste
Top

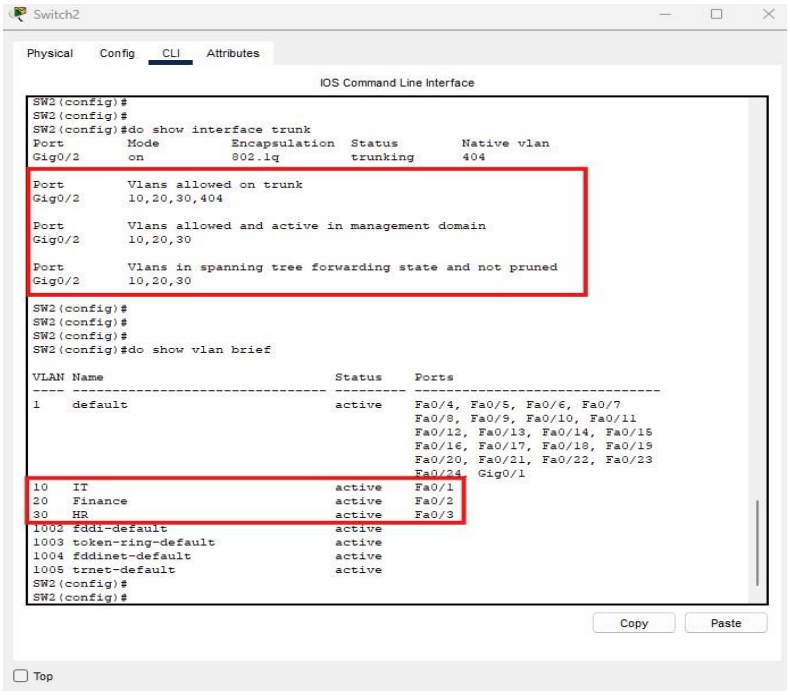


Figure 32: Native VLAN404 inactive on trunk links

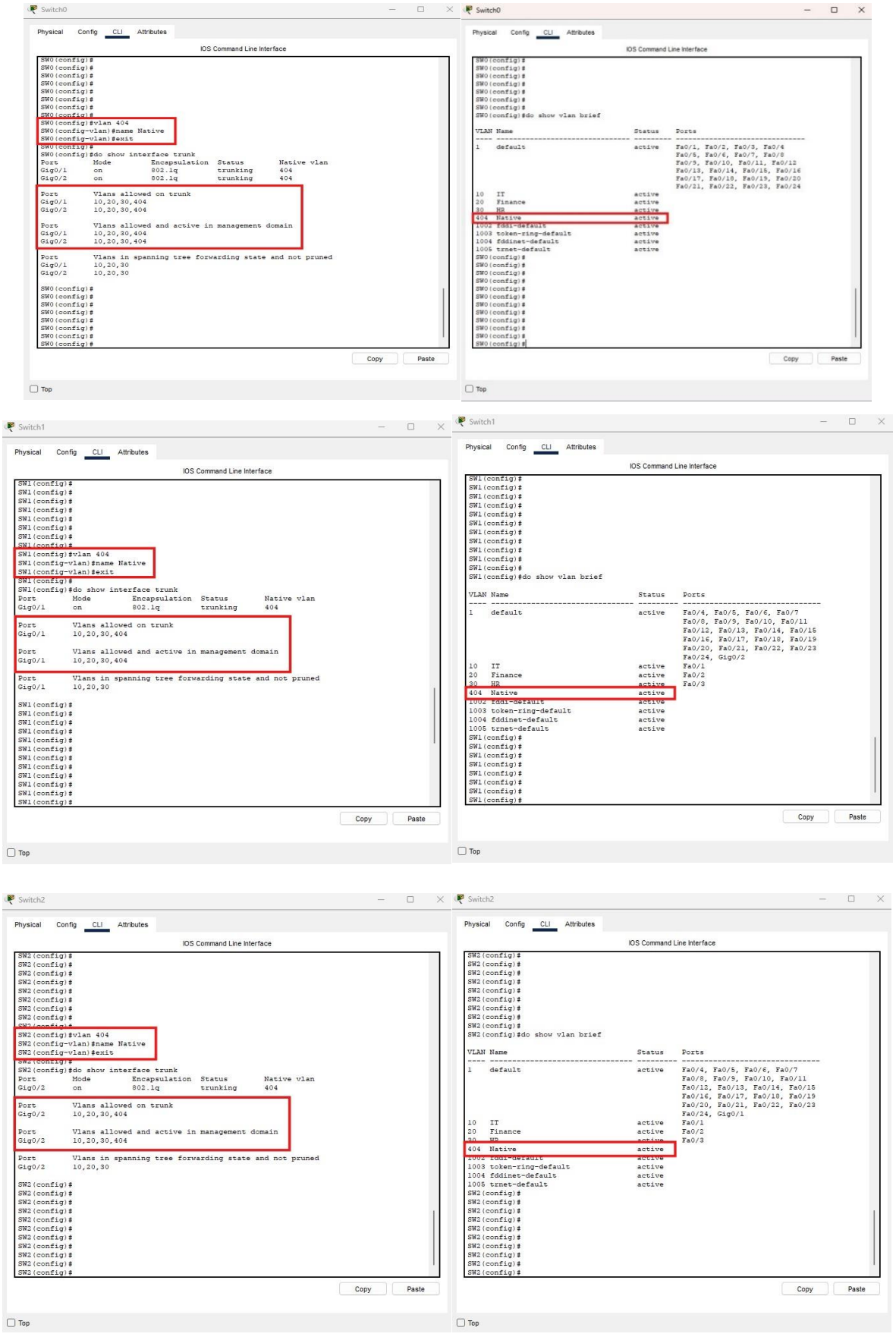


Figure 33: VLAN 404 on switches to activate native VLAN

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC1	PC4	ICMP		0.000	N	0	(edit)
	Successful	PC4	PC1	ICMP		0.000	N	1	(edit)
	Successful	PC2	PC5	ICMP		0.000	N	2	(edit)
	Successful	PC5	PC2	ICMP		0.000	N	3	(edit)
	Successful	PC3	PC6	ICMP		0.000	N	4	(edit)
	Successful	PC6	PC3	ICMP		0.000	N	5	(edit)

Figure 34: PC-PC communication with same VLAN

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Failed	PC1	PC5	ICMP		0.000	N	0	(edit)
	Failed	PC1	PC6	ICMP		0.000	N	1	(edit)
	Failed	PC2	PC4	ICMP		0.000	N	2	(edit)
	Failed	PC2	PC6	ICMP		0.000	N	3	(edit)
	Failed	PC3	PC4	ICMP		0.000	N	4	(edit)
	Failed	PC3	PC5	ICMP		0.000	N	5	(edit)

Figure 35: Inter switch VLAN communication test

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Failed	PC4	PC2	ICMP		0.000	N	0	(edit)
	Failed	PC4	PC3	ICMP		0.000	N	1	(edit)
	Failed	PC5	PC1	ICMP		0.000	N	2	(edit)
	Failed	PC5	PC3	ICMP		0.000	N	3	(edit)
	Failed	PC6	PC1	ICMP		0.000	N	4	(edit)
	Failed	PC6	PC2	ICMP		0.000	N	5	(edit)

Figure 36: Inter VLAN connectivity test

SUMMARY

CE 2.13 Working on this assessment, I planned, configured, tested, monitored and troubleshot an enterprise network by using practical network engineering principles across VLANs, PVLANs, SVIs, IPv4/IPv6 interoperability and switch-based services. I chose and used network testing and monitoring tools to assess connectivity, performance and security. I developed maintenance plans for Cisco IOS devices, monitored routing protocols and router configurations and isolated network problems across various OSI layers by analyzing MAC addressing, ARP behavior and IP routing. I tested switch to switch communication, trunking, access ports, loop prevention using STP and checked advanced services via BERT, RFC 2544 and multi stream traffic testing. I implemented and checked PVLANs and SVIs to enhance traffic segmentation and inter VLAN routing efficiency. During troubleshooting, I noticed and corrected VLAN misconfiguration, trunk inconsistencies, IP conflicts, subnet errors and native VLAN mismatches to restore stable function. This assessment enhanced my practical

capability in network planning, optimization, troubleshooting, performance analysis and security management.