BSc (Hons) Computer Networks

Advanced Networking - CIS005-3

Assignment 1 – Individual Report

Course Instructor: Mr Vibhavi Attigala

Student Name: V. Gurunivasan

Student ID: 2526303

ABSTRACT

The project is about designing and implementing a network solution which is suitable for Crescent Studios, an animation and production company for movies. The main challenge here was to provide an infrastructure that supports bandwidth-intensive applications, such as 4K video editing, CGI editing and 3D rendering, while also enforcing tight security between departments.

I have applied the concept of a segmented network architecture through the application of VLANs to logically separate the two major groups: Technical and Operations. To manage the traffic flow, I applied well-configured Access Control Lists. This ensures animators have unrestricted access, which they need for collaboration, while other departments operate in controlled environments. The network also sports a secure wireless setup with six strategically placed access points, each using WPA2 encryption. Testing shows that the system meets all operational requirements by supporting high-speed data transfer for creative work and preventing unauthorized cross-departmental access effectively.

TABLE OF CONTENTS

TABLE OF FIGURES

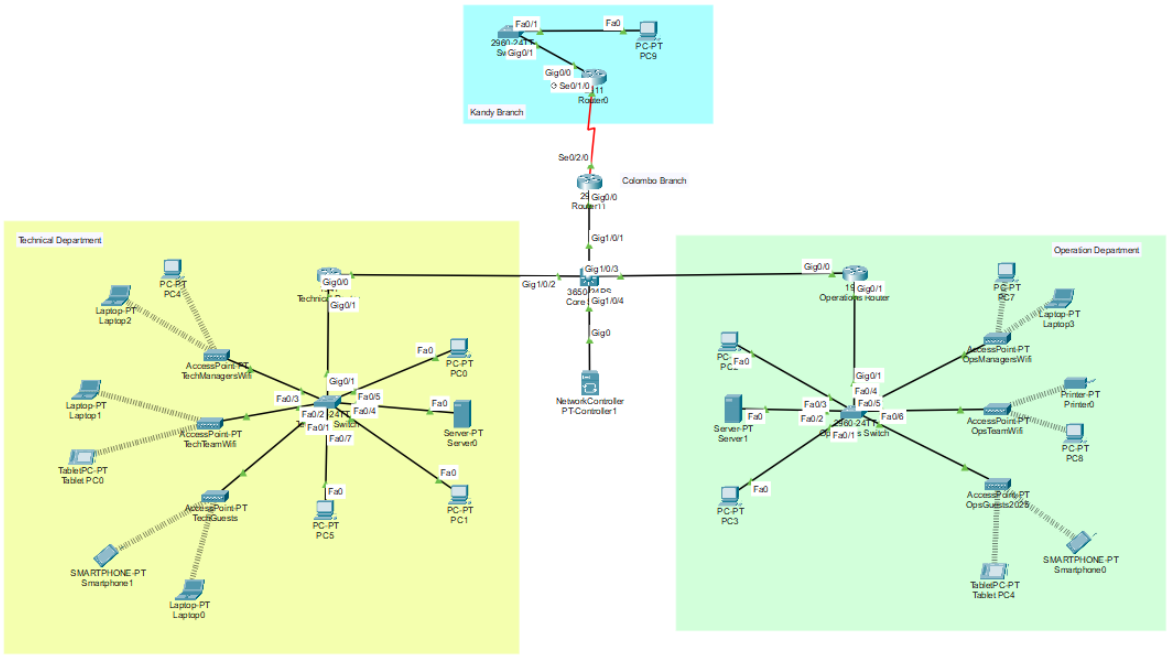
LIST OF TABLES

01. INTRODUCTION AND NETWORK DESIGN

1.1 Introduction

This report describes a proposed network design for Crescent Studios, a mid-sized creative company specializing in CGI, animation, video editing, and client operations. The organization consists of 2 branches (Kandy and Colombo) and two major departments on 2 floors on one branch (Technical and Operations) with different performance and security requirements for each. Due to increased workloads, collaborative projects, and client meetings, it's important that Crescent Studios be fitted with a modern, secure, and scalable network infrastructure design. The objective of this proposed network is to provide a high-performance office environment with advanced VLAN segmentation, inter-VLAN routing, secure switching technologies, and structured IP addressing. Primary considerations in the design include security, wireless connectivity, and easy expansion.

1.2 Network Design and Architecture



1.3 IP Addressing Scheme

Host / VLAN	Subnet	Network Address	Broadcast Address	1st Usable	Last Usable	Subnet Mask
Tech Managers - VLAN 10	192.168.1.0/24	192.168.1.0	192.168.1.255	192.168.1.1	192.168.1.254	255.255.255.0
Tech Team -VLAN 20	192.168.2.0/24	192.168.2.0	192.168.2.255	192.168.2.1	192.168.2.254	255.255.255.0
Tech Guests - VLAN 30	192.168.3.0/24	192.168.3.0	192.168.3.255	192.168.3.1	192.168.3.254	255.255.255.0
Operation Managers -VLAN 40	192.168.4.0/24	192.168.4.0	192.168.4.255	192.168.4.1	192.168.4.254	255.255.255.0
Operation Team - VLAN 50	192.168.5.0/24	192.168.5.0	192.168.5.255	192.168.5.1	192.168.5.254	255.255.255.0
Operation Guests - VLAN 60	192.168.6.0/24	192.168.6.0	192.168.6.255	192.168.6.1	192.168.6.254	255.255.255.0
Infrastructure- VLAN 99	192.168.99.0/24	192.168.99.0	192.168.99.255	192.168.99.1	192.168.99.254	255.255.255.0

Table 1_Colombo Office VLAN Subnets and IP Addressing Scheme

Link	Subnet	Network Address	Broadcast Address	1st Usable	Last Usable	Branch / Details
Main Router <-> Branch Router	10.0.0.0/30	10.0.0.0	10.0.0.3	10.0.0.1	10.0.0.2	Main Branch to Kandy Branch
Core Router	10.0.0.1/30	10.0.0.1	10.0.0.3	10.0.0.1	10.0.0.1	Main Router Interface
Branch Router	10.0.0.2/30	10.0.0.2	10.0.0.3	10.0.0.2	10.0.0.2	Kandy Branch Router Interface

Table 2_Connection Between Colombo Branch (Main Router) and Kandy Branch (Branch Router)

Host / LAN	Subnet	Network Address	Broadcast Address	1st Usable	Last Usable	Branch
Branch Router LAN	192.168.200.0/24	192.168.200.0	192.168.200.255	192.168.200.1	192.168.200.254	Kandy Branch

Table 3_Branch Office Scheme_Kandy Branch

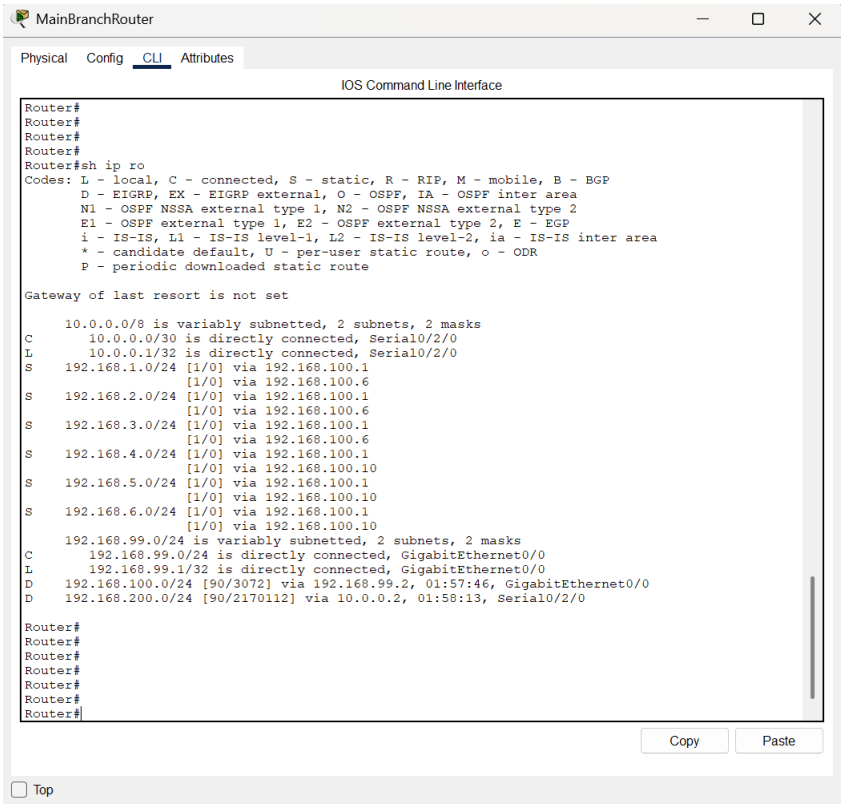


Figure 1_MainRouterRouting_ColomboBranch

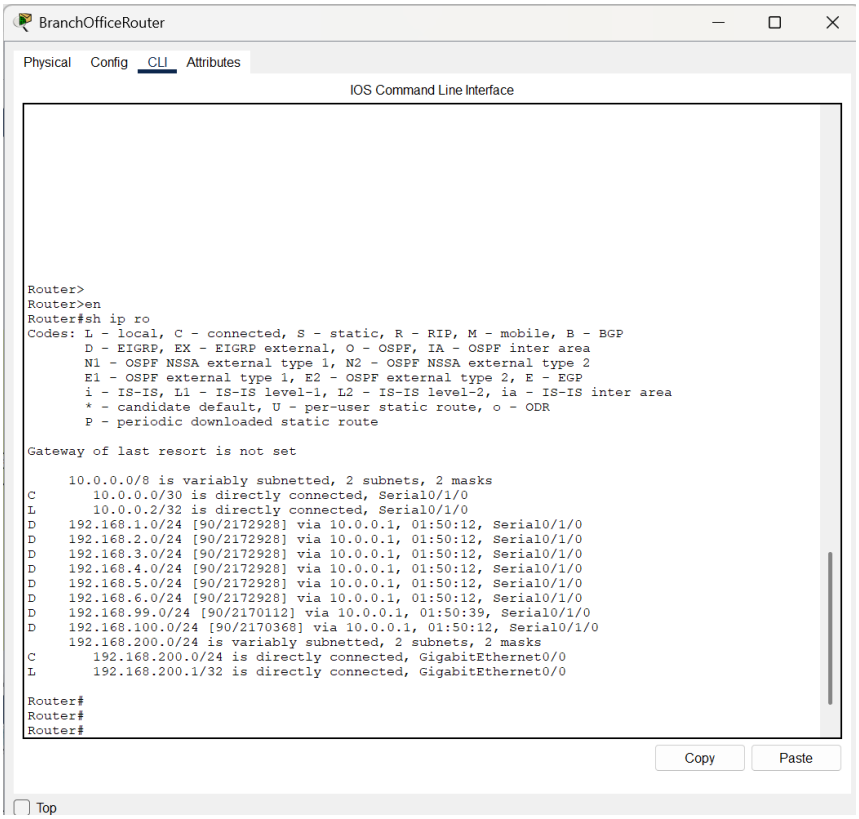


Figure 2_Routing On Kandy Branch

02. METHODOLOGY AND RESULTS

2.1 VLAN Configurations

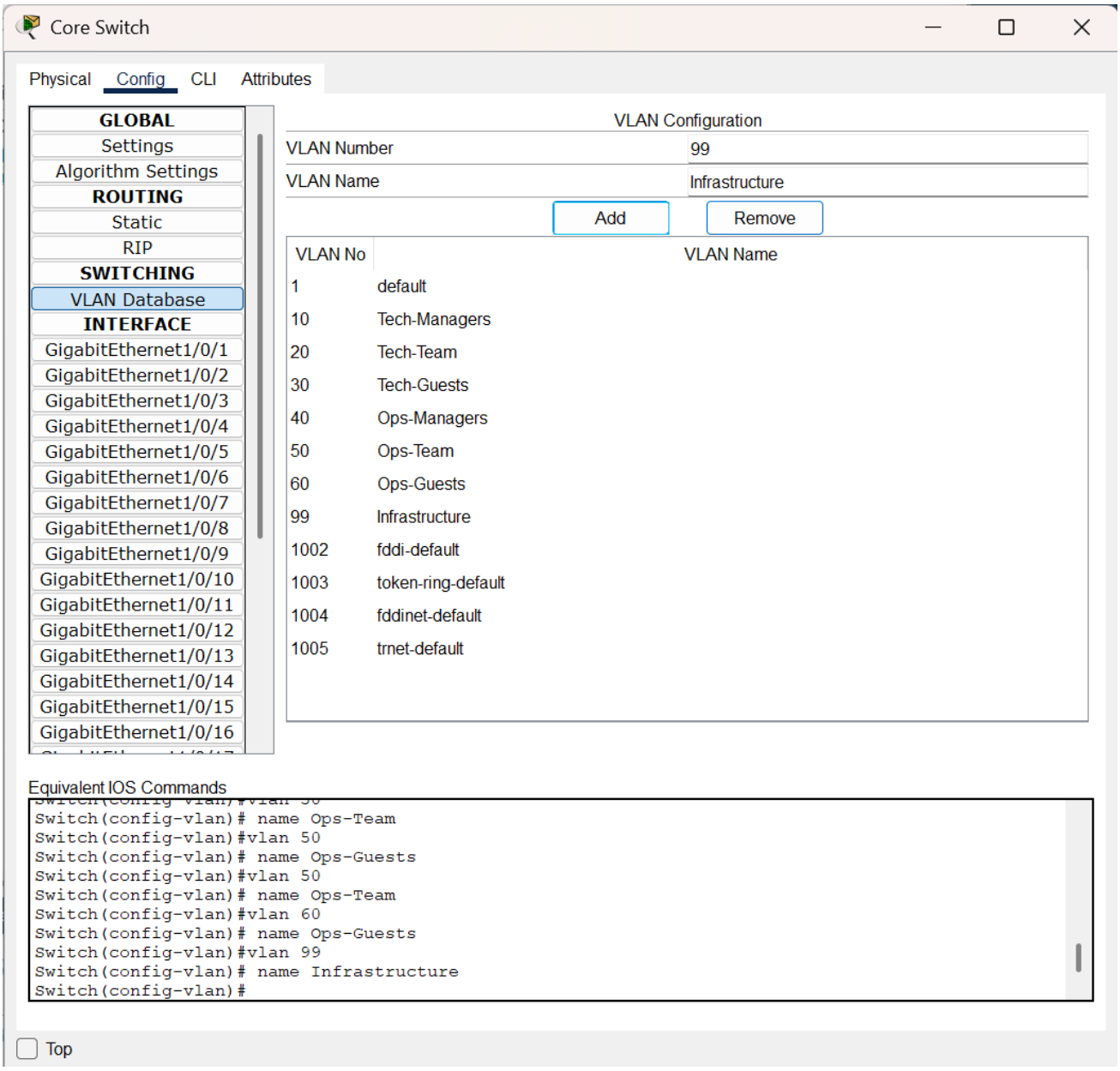


Figure 3_VLAN Configurations

2.2 Trunk Port Configurations

```
Switch>
Switch>en
Switch#
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig1/0/1    on           802.1q         trunking      99

Port        Vlans allowed on trunk
Gig1/0/1    10,20,30,40,50,60,99

Port        Vlans allowed and active in management domain
Gig1/0/1    10,20,30,40,50,60,99

Port        Vlans in spanning tree forwarding state and not pruned
Gig1/0/1    10,20,30,40,50,60,99

Switch#
```

Figure 4_ Trunk Configuration On Multilayer Switch

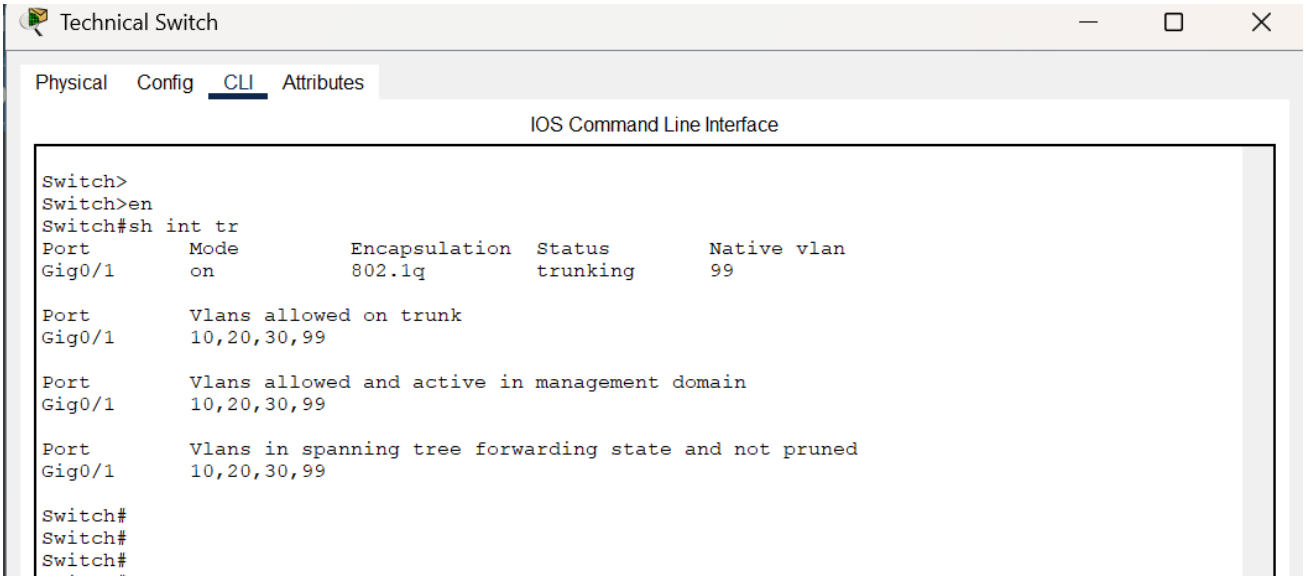


Figure 5_ Trunk Configuration on Technical Department Switch

2.3 DHCP Configurations

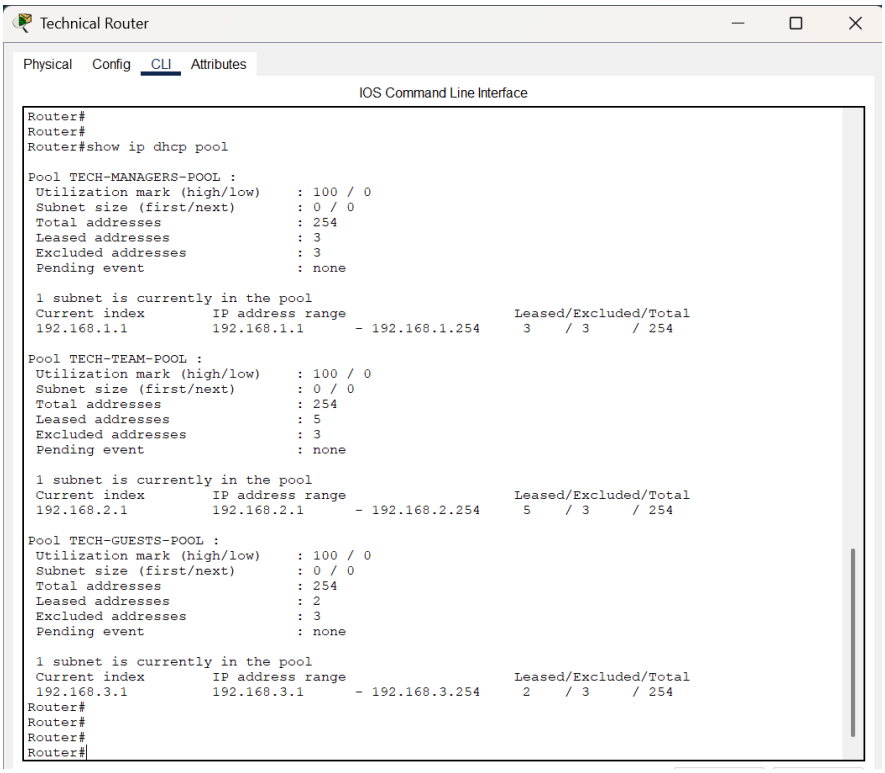


Figure 6_DHCP Configuration on Technical Department Router

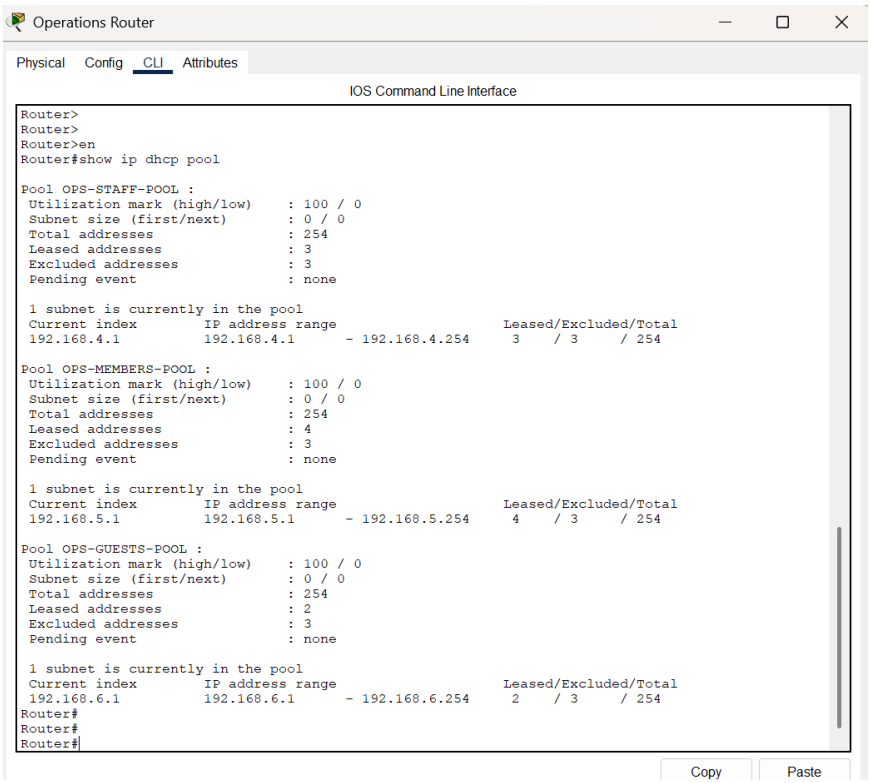


Figure 7_DHCP Configuration on Operations Department Router

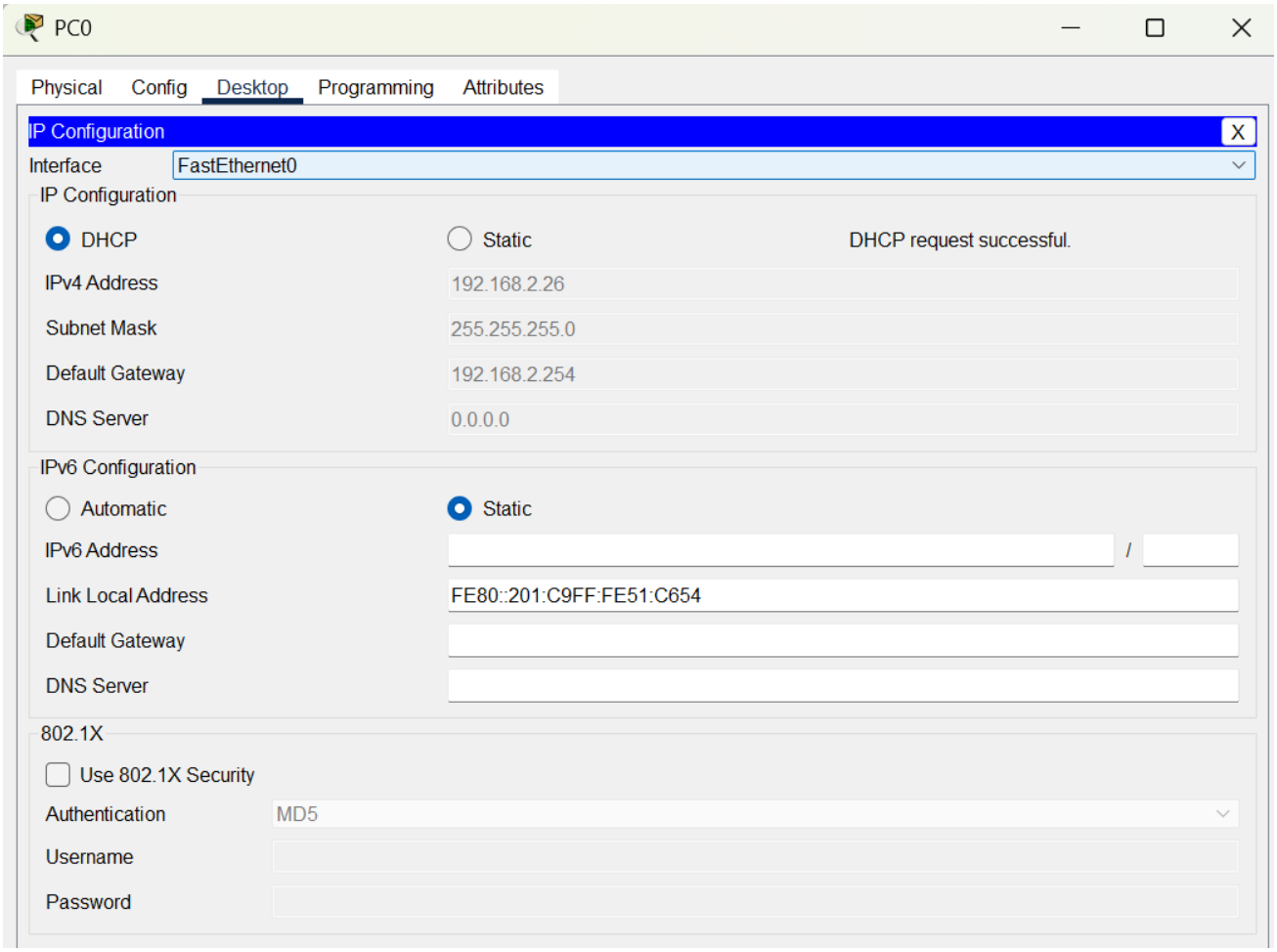


Figure 8_ DHCP Successful

2.4 Wireless Access Points Implementation

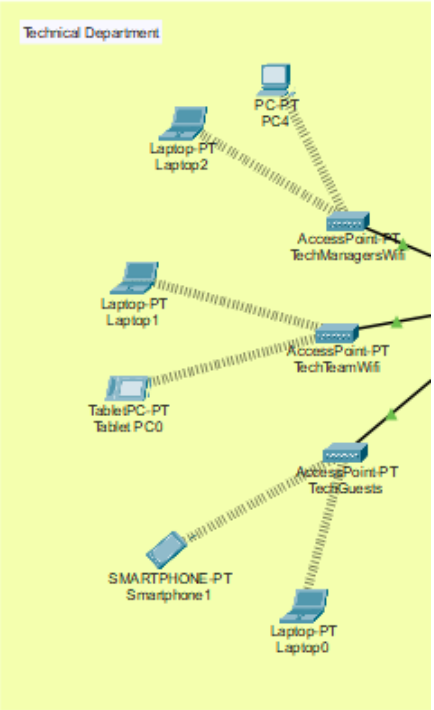


Figure 9_Technical Department APs for each type of user

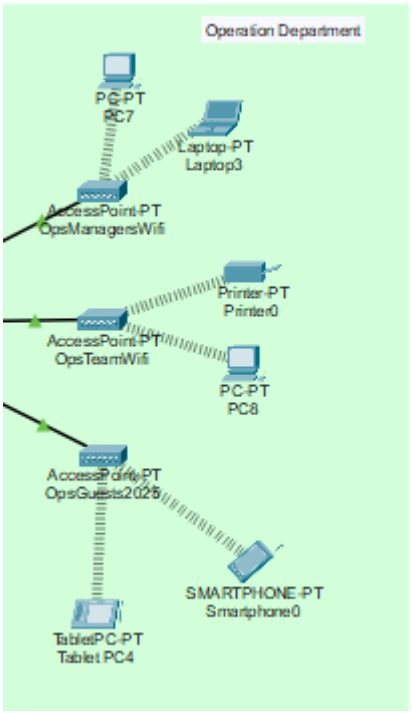


Figure 10_AP on Operations Department for each user

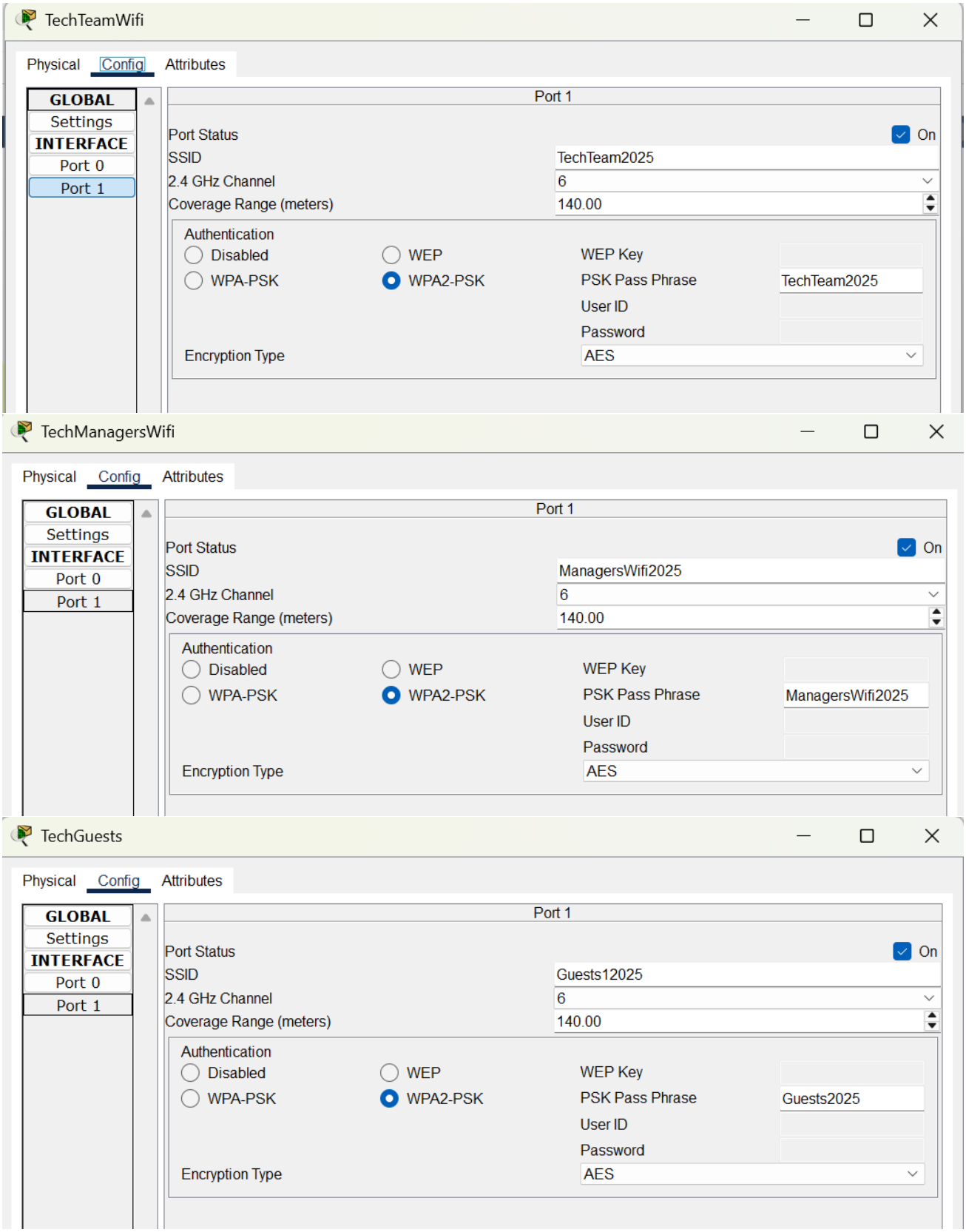


Figure 11_Setting Up SSIDs and WPA2-PSK for the Technical Department

2.5 Network Controller Setup

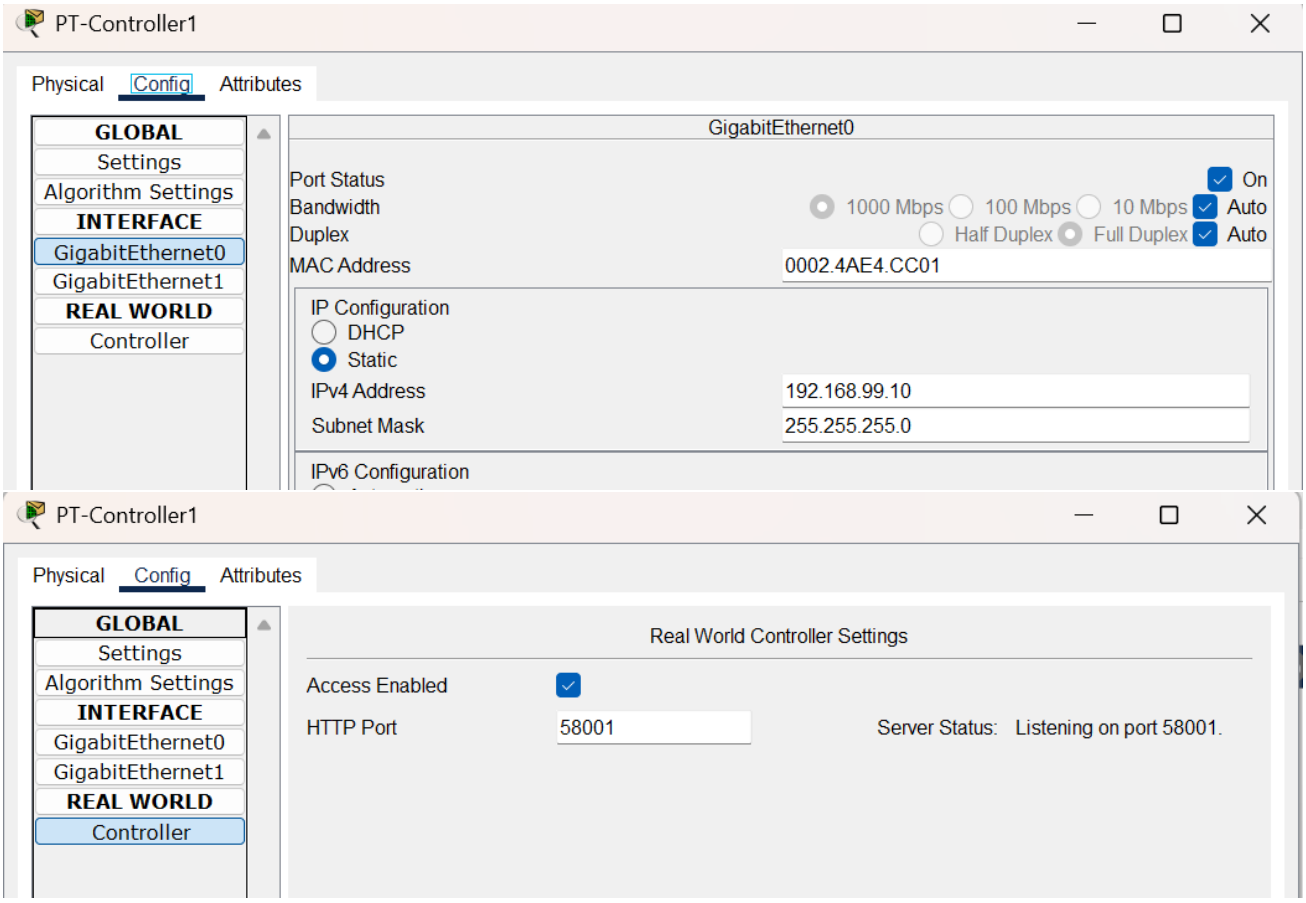


Figure 12_Setting Up the Network Controller

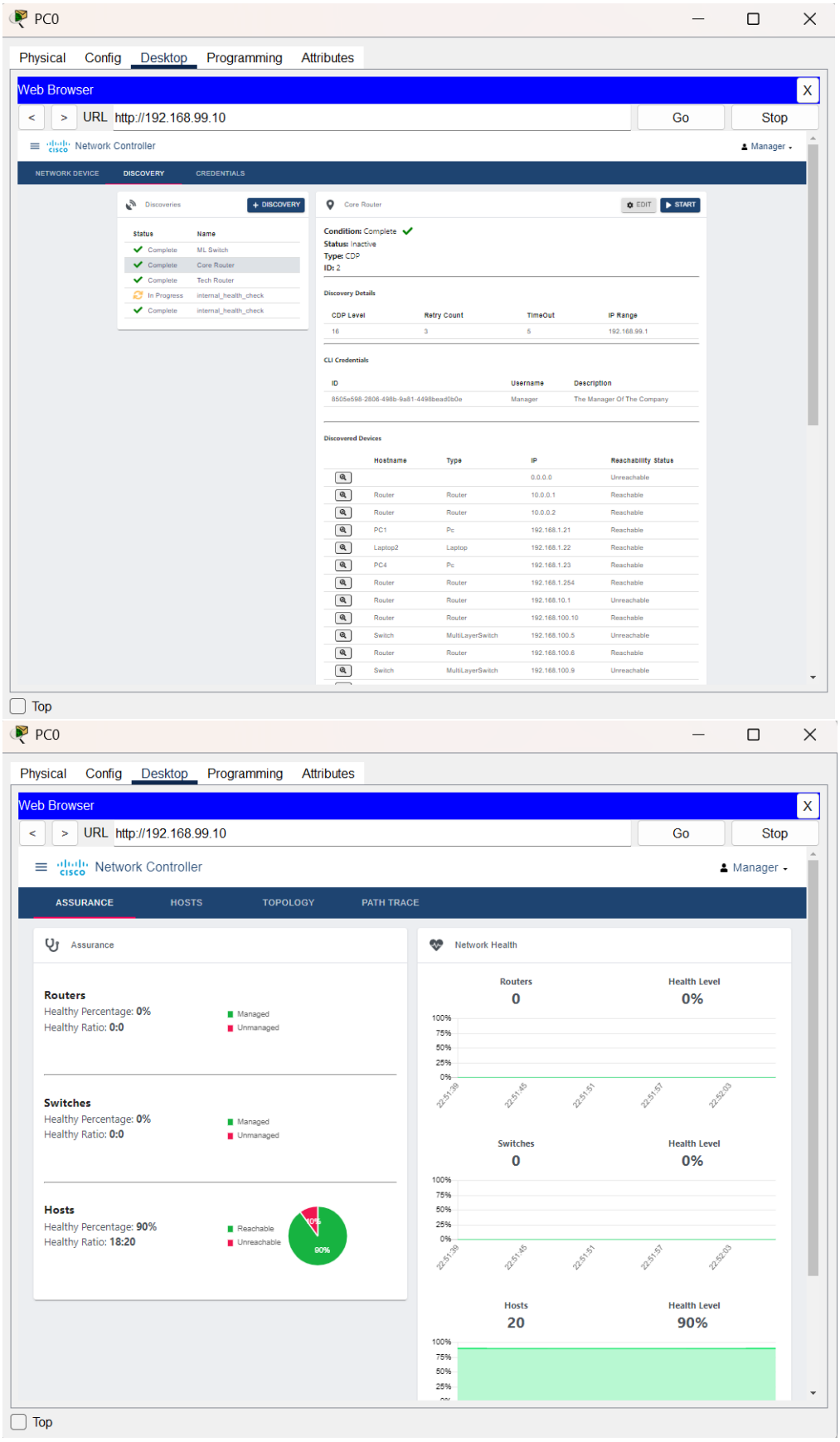


Figure 13_ Network Controller Discoveries

2.6 ACL Configuration

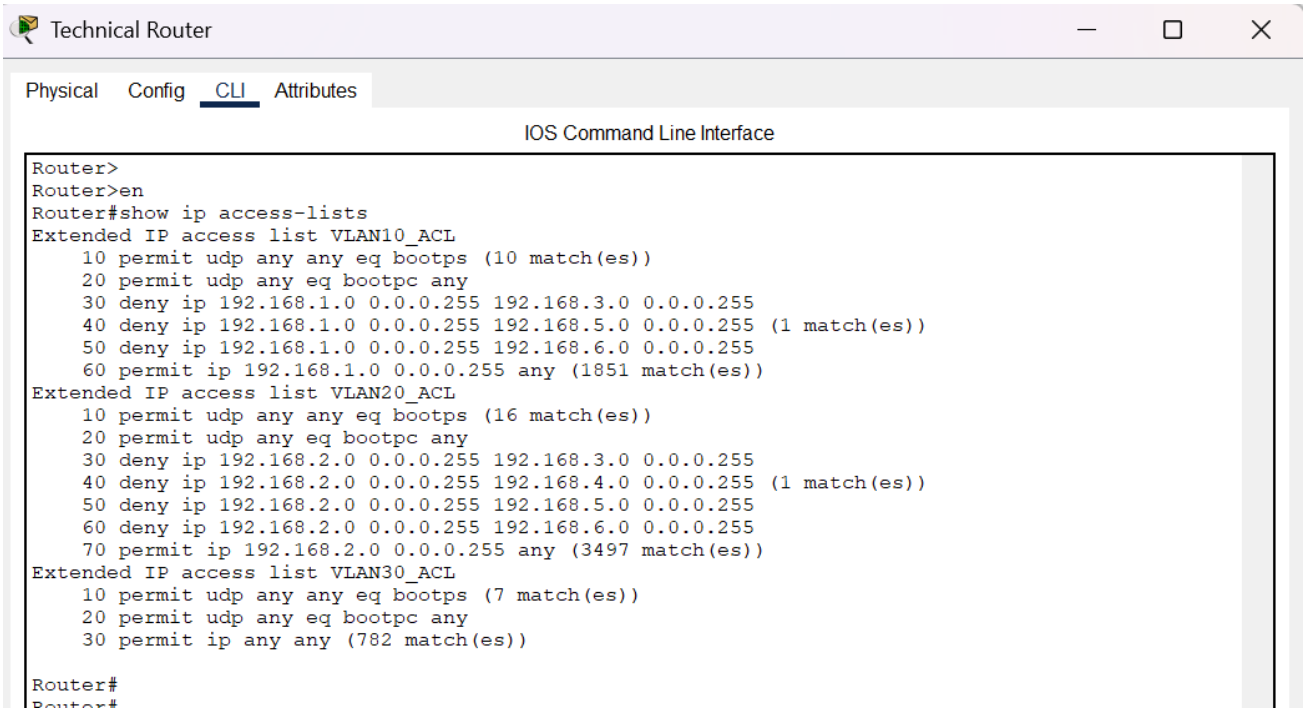


Figure 14_ ACL Configuration on Technical Router

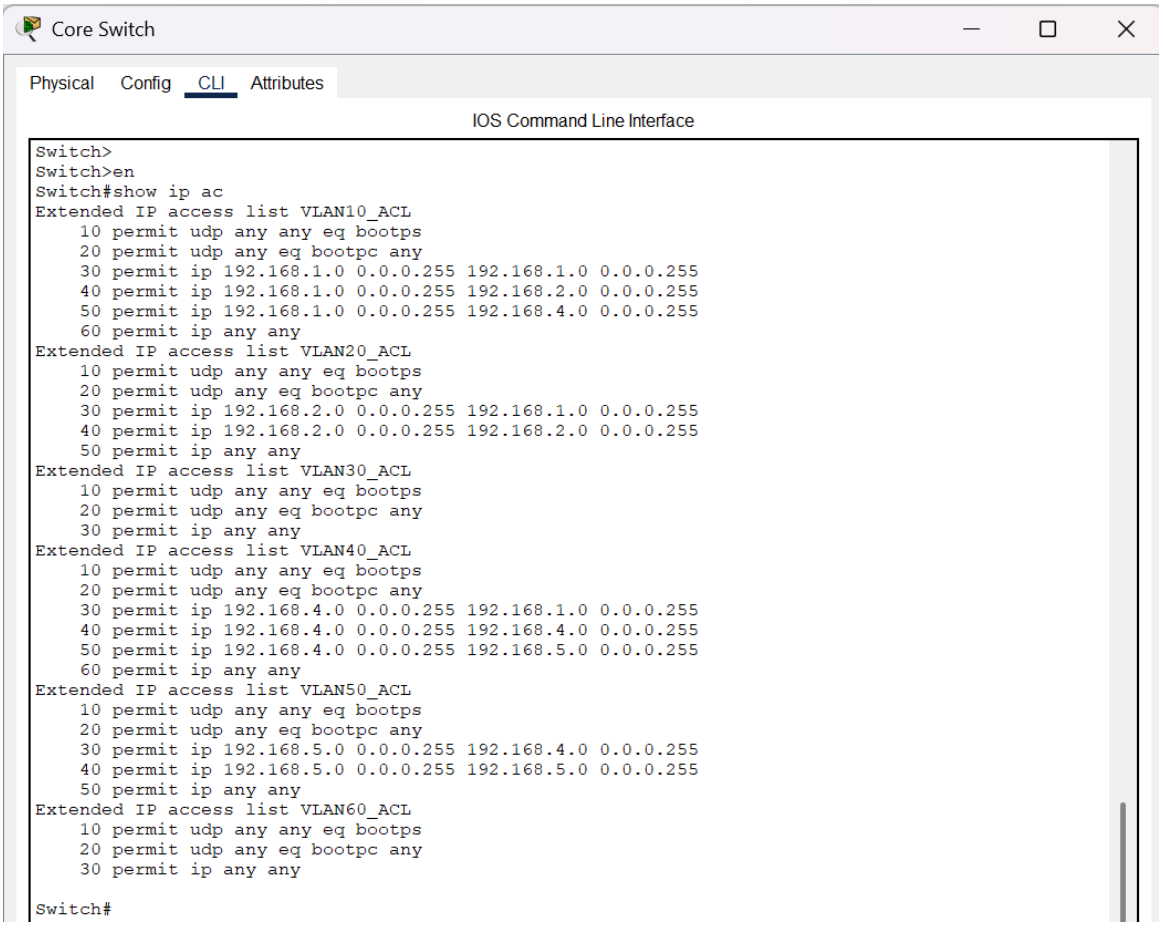


Figure 15_ ACL Configuration on Core Switch

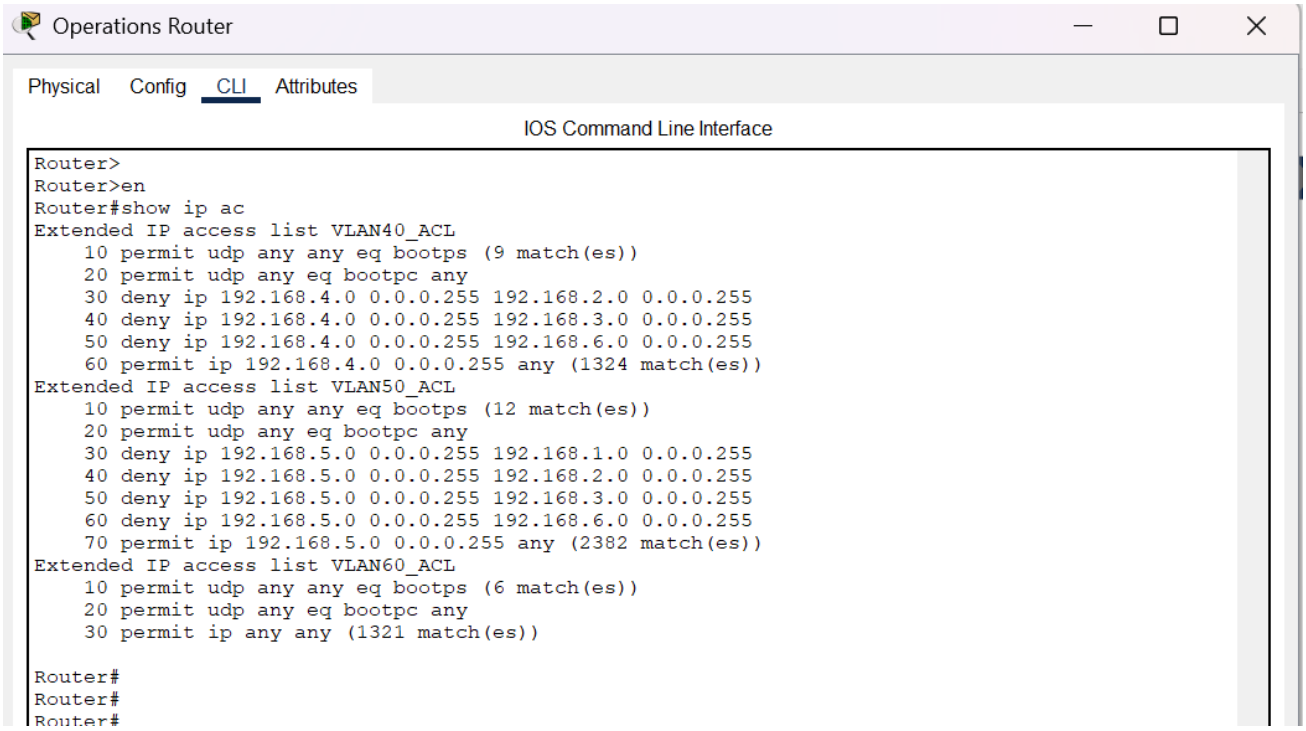


Figure 16_ ACL on Operation Router

2.7 EIGRP Configurations

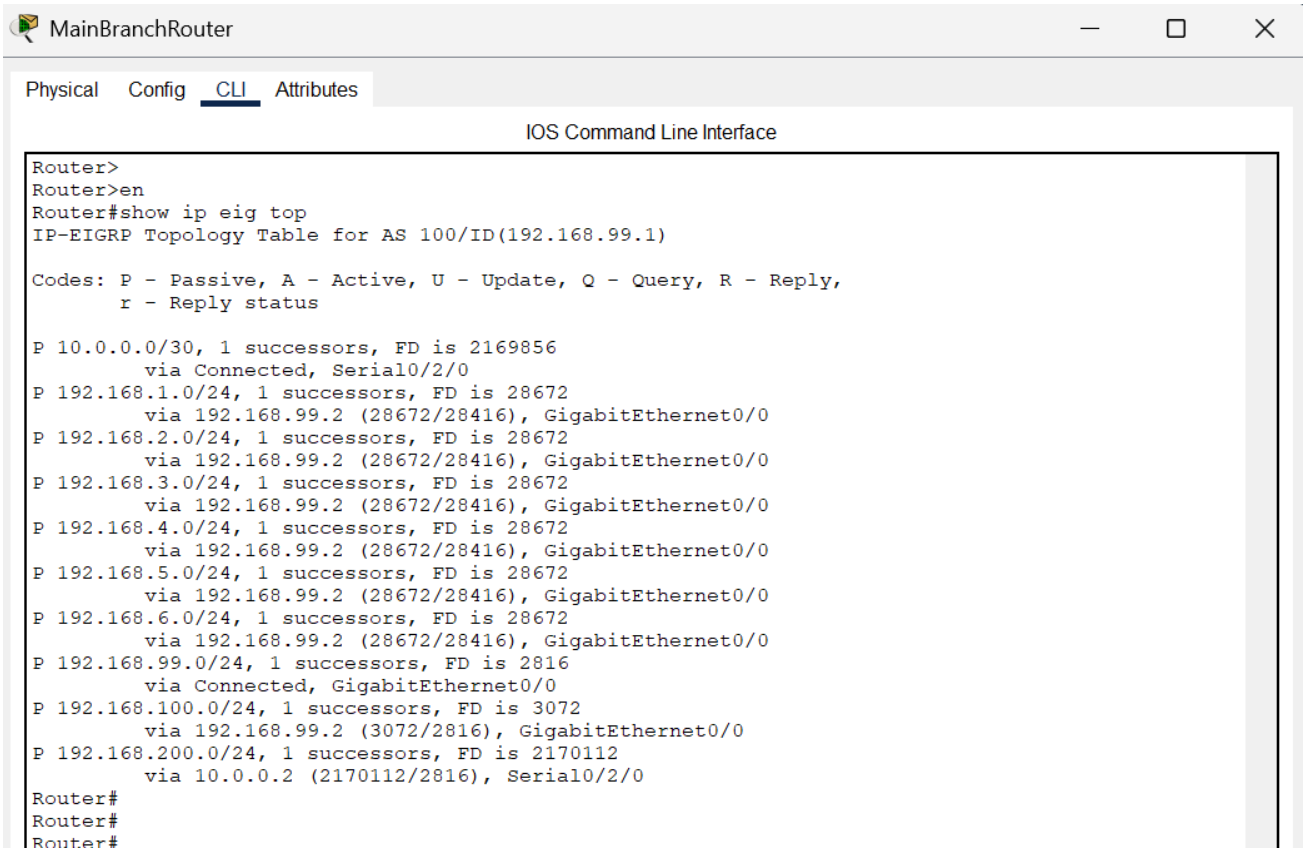


Figure 17_ EIGRP Topology Taken From the Main Branch Router

2.8 Connectivity Testing and Results

VLAN / ACL	ALLOWED COMMUNICATION	DENIED COMMUNICATION	REASON / JUSTIFICATION
VLAN 10 – TECH MANAGERS	VLAN 10, VLAN 20, VLAN 40	VLAN 30, VLAN 50, VLAN 60	Allow full access to team members and Ops management. Block guests and non-related Ops VLANs to maintain internal security.
VLAN 20 – TECH MEMBERS	VLAN 10, VLAN 20	VLAN 30, VLAN 40, VLAN 50, VLAN 60	Allow collaboration within Tech department. Restrict access to other departments and guests.
VLAN 30 – TECH GUESTS / CLIENTS	Internet only	VLAN 10, VLAN 20, VLAN 40, VLAN 50, VLAN 60	Limit guest access to Internet. Prevent internal resource access.
VLAN 40 – OPERATIONS MANAGERS	VLAN 40, VLAN 50, VLAN 10	VLAN 20, VLAN 30, VLAN 60	Allow Ops staff and management to collaborate internally and with Tech managers. Restrict unrelated Tech members and guests.
VLAN 50 – OPERATION MEMBERS (HR/FINANCE)	VLAN 40, VLAN 50	VLAN 10, VLAN 20, VLAN 30, VLAN 60	Allow internal Ops collaboration. Restrict Tech VLANs and guest access.
VLAN 60 – OPERATION GUESTS / CLIENTS	Internet only	VLAN 10, VLAN 20, VLAN 30, VLAN 40, VLAN 50	Limit external clients to Internet. No access to internal systems.
VLAN 99 – INFRASTRUCTURE	All VLANs (10–60)	N/A	Full access for management and IT infrastructure to monitor and maintain all departments.

Table 4_Allowed and Denied Communications Between the Networks and Justification

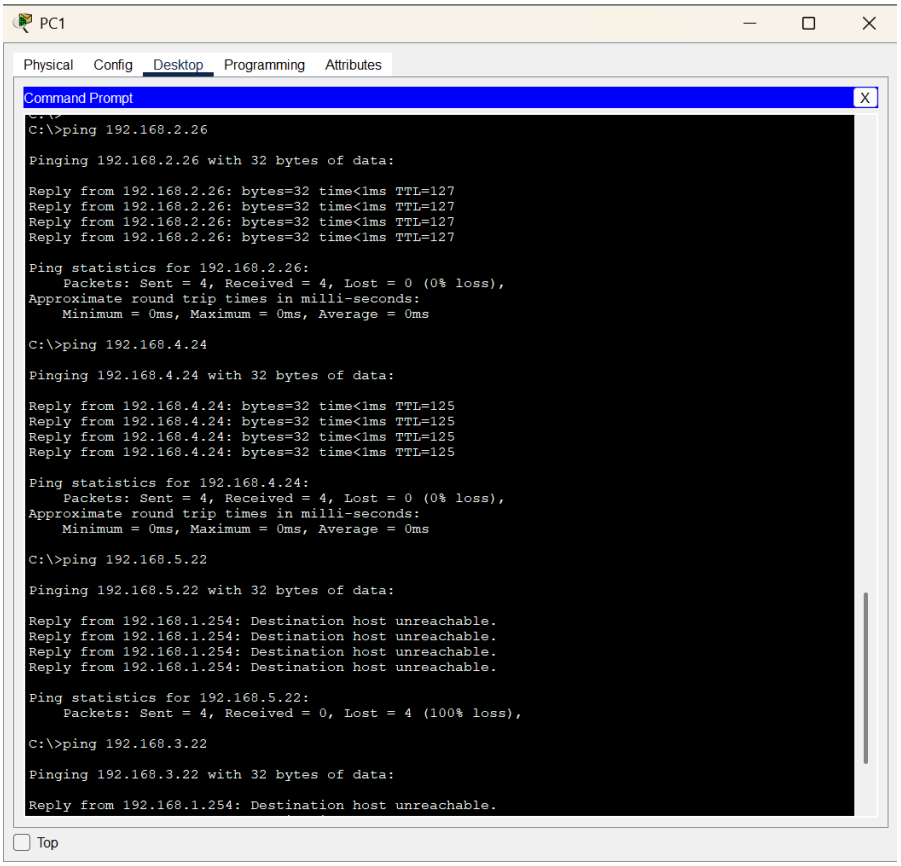


Figure 18_ Ping tests from a device in VLAN 10

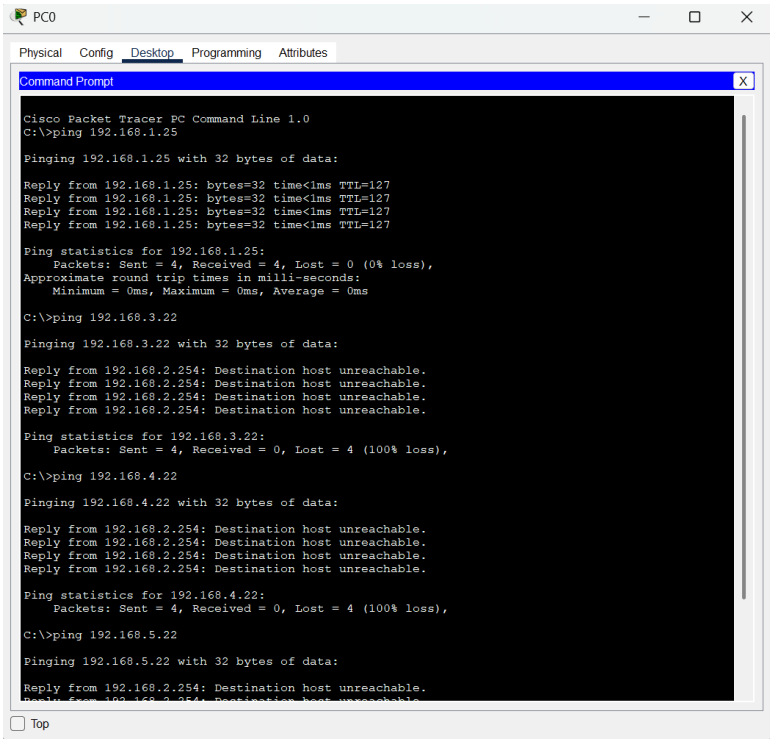


Figure 19_Ping test from a device in VLAN 20

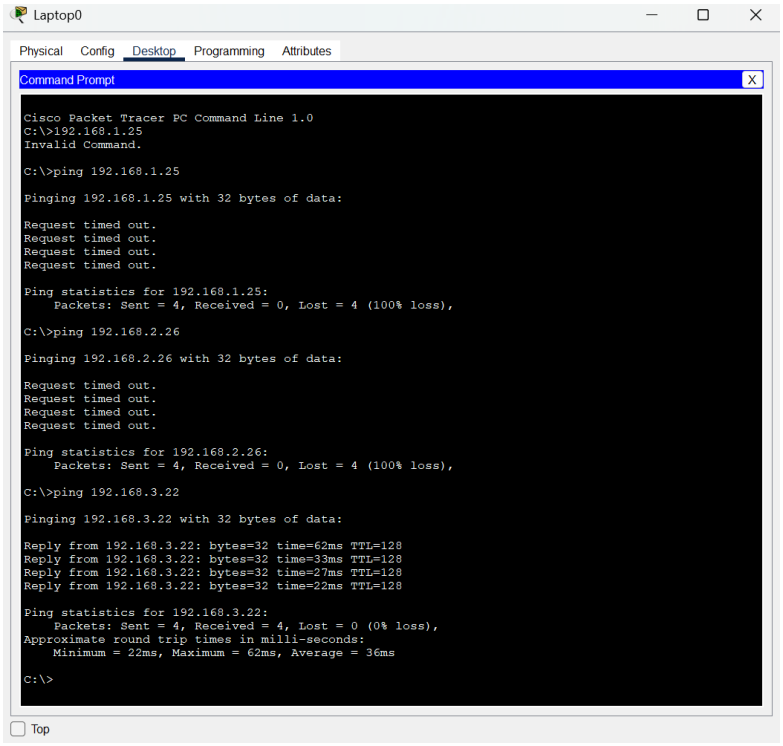


Figure 20_Ping Test from a Device in VLAN 30

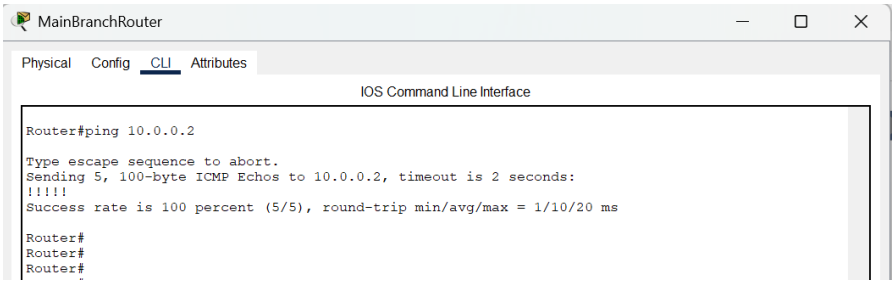


Figure 21_ Testing Connectivity from Router in Colombo Branch to Router in Kandy Branch

03. DISCUSSION AND CONCLUSIONS

3.1 The Network Design

The network design used in Crescent Studios was used to address the challenges in media production environments. In contrast to typical office networks, an animation studio needs high performance for huge file transfers, along with strict security for the valuable intellectual property. A clear boundary is maintained among the three layers (core, distribution, and access) to prevent traffic from impacting administrative operations while ensuring defined security zones between creative and business data. This approach ensures that 4K video editing sessions remain smooth even at peak network usage while simultaneously protecting unreleased content through structured segmentation.

3.2 VLAN Segmentation Strategy

The reason why there were 6 VLANS is because it was necessary to not disrupt the workflow of the company. Technical teams of animators and visual effects artists need shared access to rendering clusters and network-attached storage, so they must be grouped across VLANs 10 through 20. At the same time, full isolation of guest networks in VLANs 30 and 60 protects production assets during client reviews and visits. This level of granularity shows how creative organizations in the modern world balance collaboration needs with security requirements.

3.3 IP Addressing Reasoning

The decision to use multiple Class C networks is based on operational efficiency rather than the theoretical optimization of address space. In real IT support environments, this greatly reduces resolution time when troubleshooting network issues because a device's IP address immediately identifies the department and function. This practice is quite common in medium enterprises where operational simplicity weighs stronger than perfect address utilization.

3.4 How Does Packet Tracer Limitations Affect Wireless Implementation?

This wireless design shows large gaps in simulation capabilities compared to real-world deployment. Packet Tracer is unable to represent multi-SSID enterprise access points, which forces us to use different devices for each wireless network. What this means is that our wireless design will show conceptual separation but not reflect the efficiency of the hardware or the advanced features found in actual studio deployments.

3.5 Why Use Serial Connections Between the Branches?

While selecting the serial connections for the branch offices, this shows that there are, in fact, specific real-world scenarios where leased lines make more sense. Even though SD-WAN and MPLS are modern alternatives, serial links-such as T1/E1 circuits-offer bandwidth immune to congestion over the public internet, which is important for transferring high-bandwidth media files between studio locations. Physical isolation from the public networks inherently provides security benefits, and for organizations with predictable inter-site traffic patterns, a leased line often proves more cost-effective than the equivalent managed services. This represents a solution that shows network design must consider the specific business needs rather than automatically choosing the newest technology.

3.6 What Alternative Technologies Were Considered but Rejected?

Several other design approaches were reviewed and discarded in arriving at the final design. OSPF was initially considered instead of EIGRP but proved to have slower convergence times critical for large file transfers. A single network subnetting approach was considered and then discarded in favour of multiple Class C networks for ease of operational management. Cloud-only wireless controllers were considered but more traditional on-premises management was selected for reliability of media transfer scenarios.

3.7 How does this design address operational challenges?

The network architecture explicitly targets weak points of an animation studio, such as bottlenecks in large file transfers, needs for collaborative workflow, and protection of intellectual property. Branch connectivity enables remote collaboration across locations. The security framework protects unreleased content yet permits necessary communication across departments. Each element addresses real operational challenges faced by media production companies rather than just generic best practices for networking.

04. REFERENCES

Cisco Systems (2023) EIGRP Configuration Guide, Cisco IOS Release 15M&T. Available at: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/15-mt/ire-15-mt-book.html (Accessed: 20 November 2025).

Cisco Systems (2023) VLAN Configuration Guide, Cisco IOS XE Release 3SE. Available at: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-9/configuration_guide/vlan/b_169_vlan_9500_cg.html (Accessed: 5 November 2025).

Tanenbaum, A. and Wetherall, D. J. (2021) Computer Networks. 6th edition. Pearson.

Wi-Fi Alliance (2023) WPA2 Security for Wireless Networks. Available at: https://www.wi-fi.org/discover-wi-fi/security (Accessed: 15 November 2025).

Cisco Systems (2023) DHCP Configuration Guide, Cisco IOS Release 15M&T. Available at: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-mt/dhcp-15-mt-book.html (Accessed: 10 November 2025).

05. APPENDICES

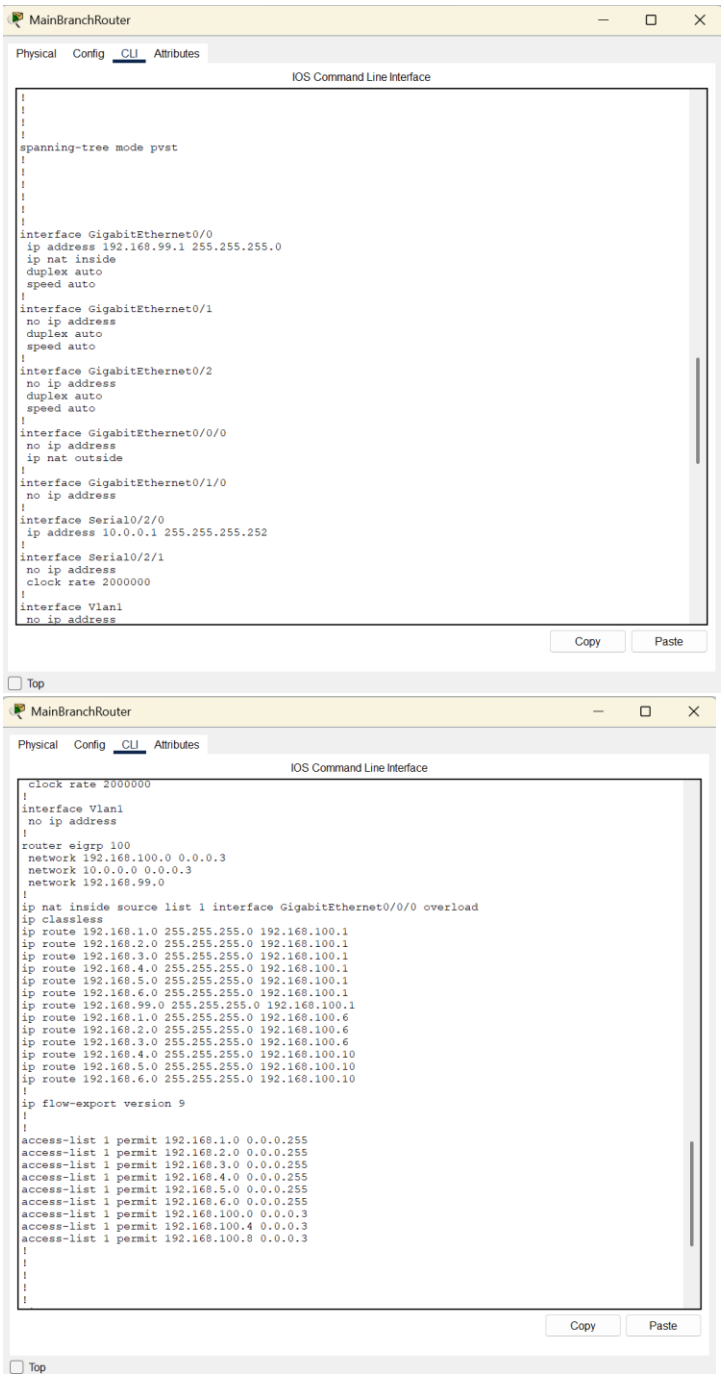


Figure 22_Colombo Main Router Running Config

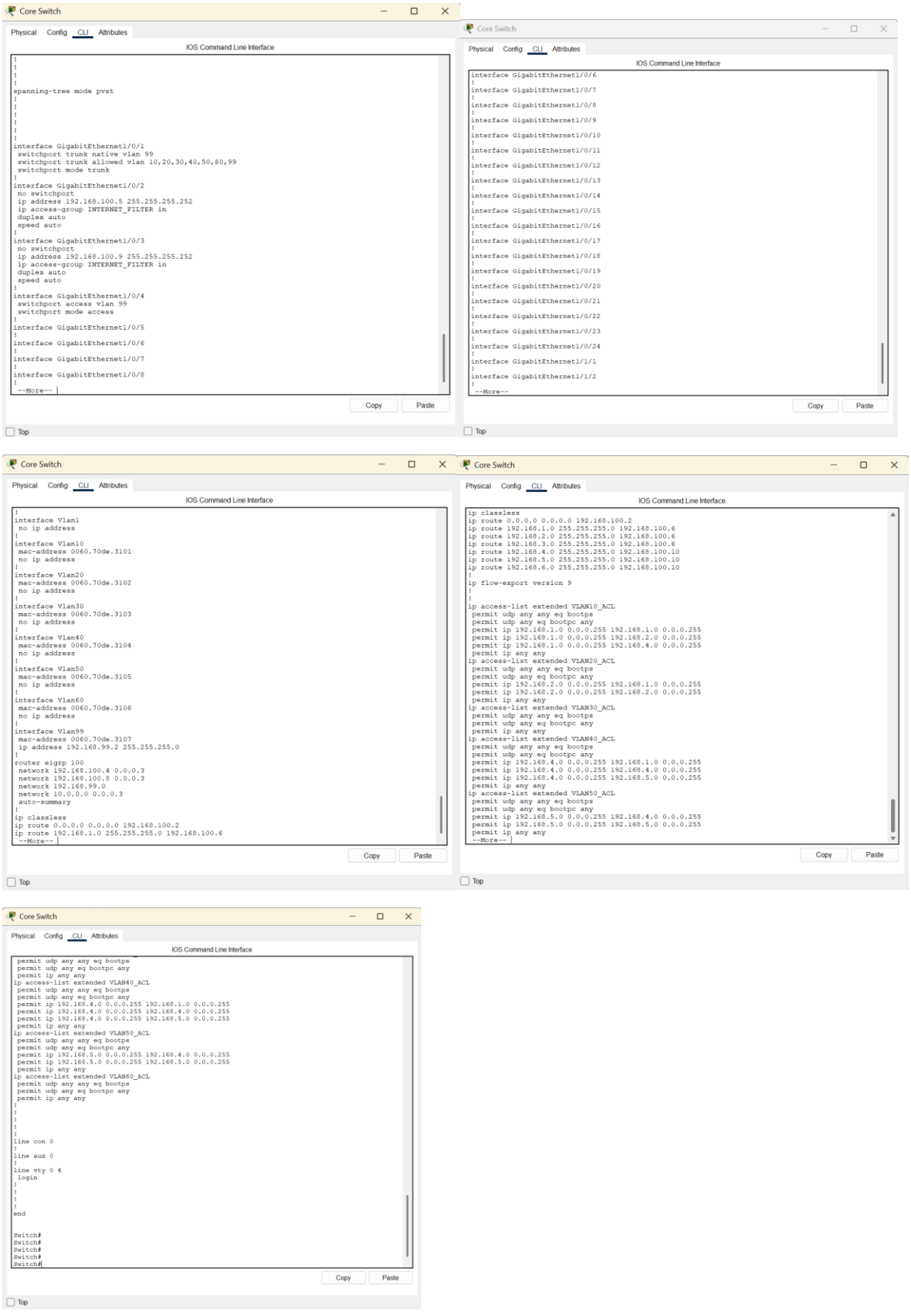


Figure 23 Multilayer Switch Running Configurations

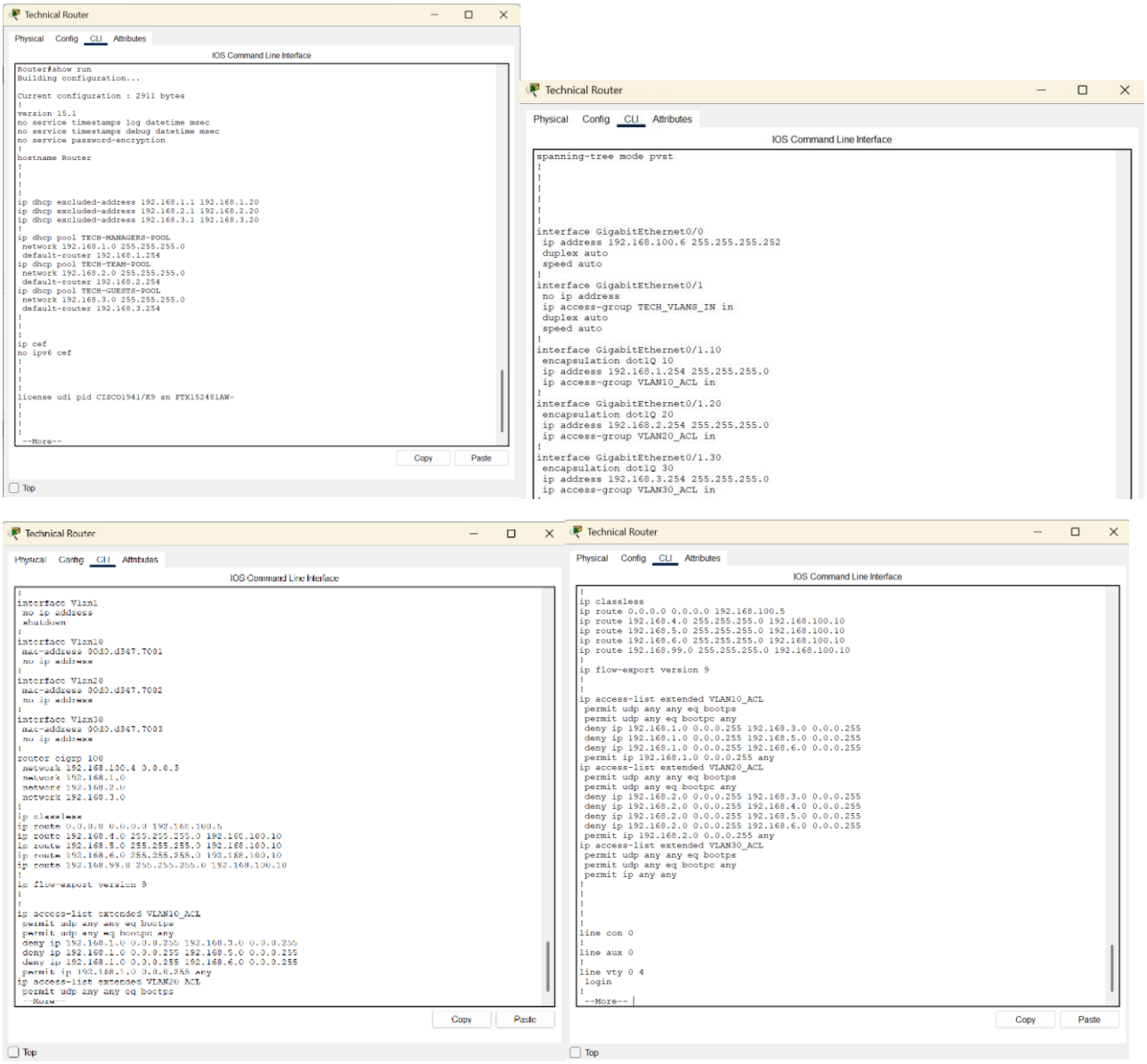


Figure 24_Technical Department Router Running Configurations

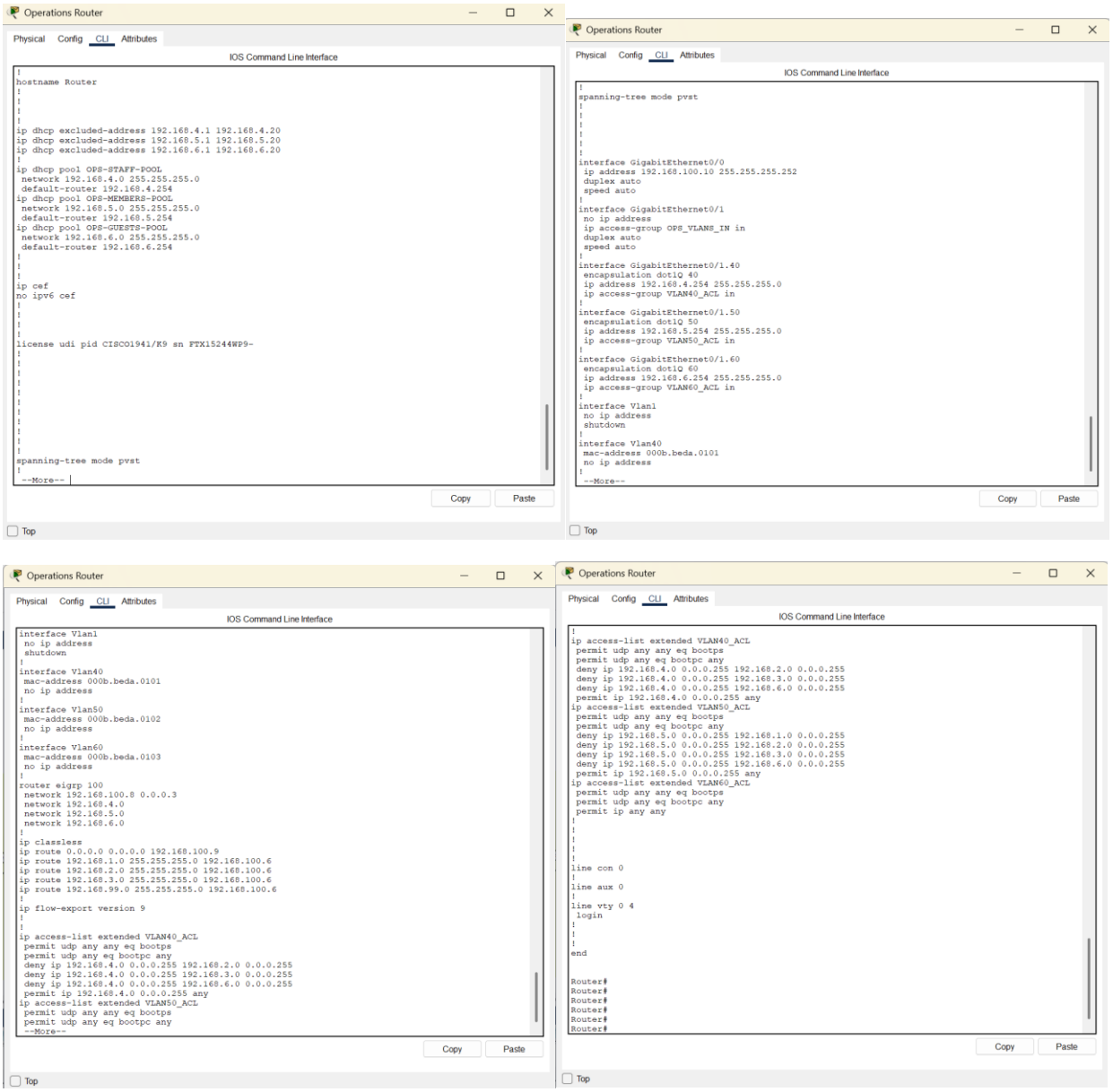


Figure 25_Operations Department Router Running Configuration

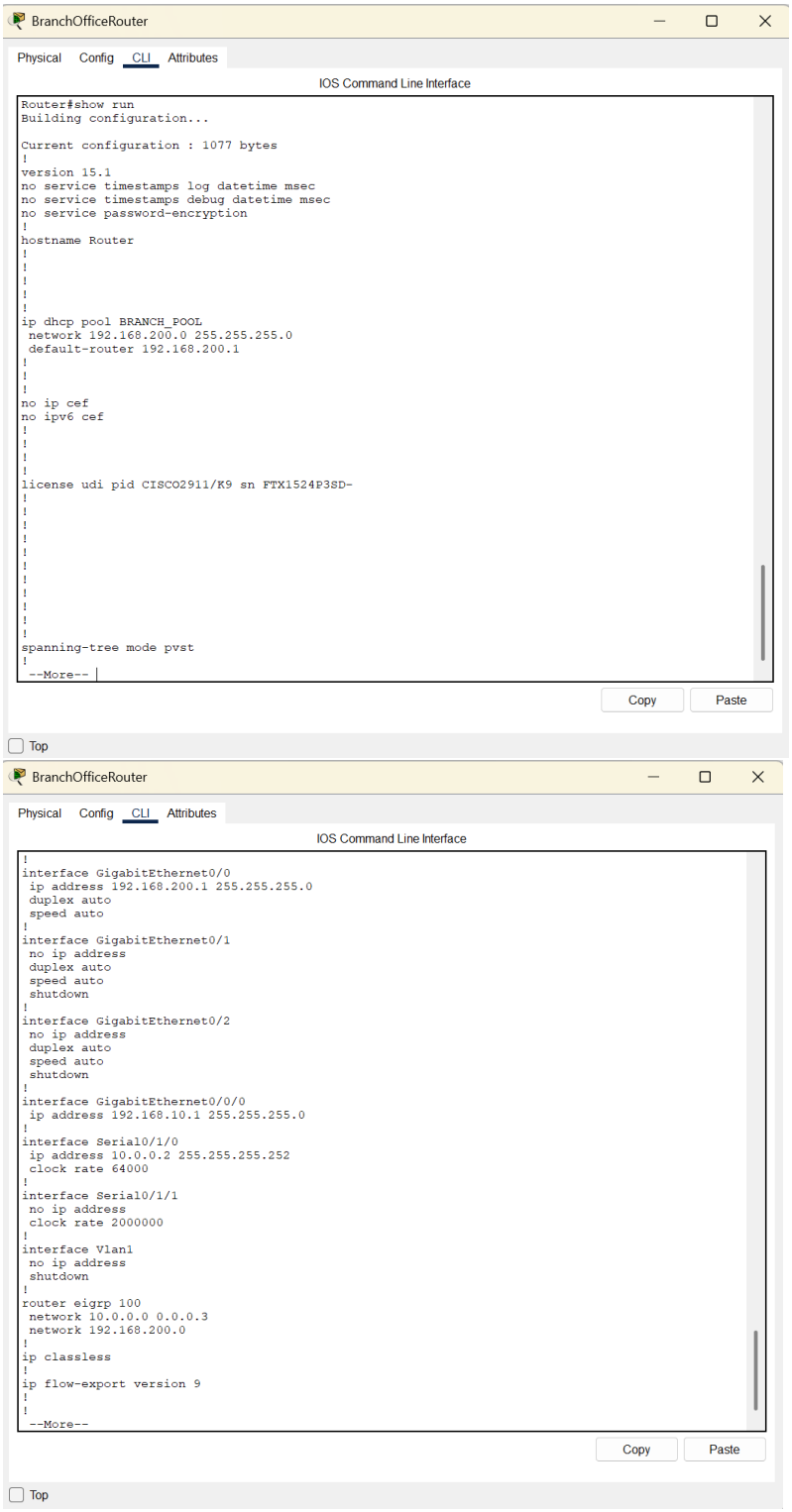


Figure 26_Kandy Branch Office Core Router Running Configurations