**INWK-6112 COURSE PROJECT**

By

SAI BHARATH REDDY CHODAVARAM (B00981831)

HARIJI MURARI PADMALATHA (B00983950)

KATHIRESAN SONAIMUTHU (B00942289)

Submitted in partial fulfilment of the requirements for the degree of

MASTER OF ENGINEERING

Major Subject: Internetworking

at

DALHOUSIE UNIVERSITY

Halifax, Nova Scotia

June, 2024

# **INDIVIDUAL CONTRIBUTIONS**

## **GROUP MEMBERS:**

**Chodavaram Sai Bharath Reddy (B00981831):**

* Physical Topology
* Configuratuion – Vlans(20, 30, 40, 50), Intervlan Routing, Trunking, Routing Protocol(RIP), Ip-addressing for all devices
* All Test plans
* Report - Chapter 3 and Chapter 4
* PPT – Configuration and Results

**Hariji Murari Padmalatha (B00983950):**

* Configuration - Created Two Vlans 100 and 200
* Report – Chapter 1 to Chapter 2.2
* PPT

**Kathiresan Sonaimuthu (B00942289):**

* Logical Topology
* Report – Chapter 2.3 to Chapter 2.10
* Organizing the team

**TABLE OF CONTENTS**

[**INDIVIDUAL CONTRIBUTIONS** 2](#_Toc168267845)

[**GROUP MEMBERS:** 2](#_Toc168267846)

[**EXECTIVE SUMMARY** 4](#_Toc168267847)

[**CHAPTER 1** 5](#_Toc168267848)

[**1.1 COMPANY OVERVIEW:** 5](#_Toc168267849)

[**1.2 NETWORK REQUIREMENTS:** 5](#_Toc168267850)

[**CHAPTER 2** 6](#_Toc168267851)

[**2.1 LOGICAL TOPOLOGY:** 7](#_Toc168267852)

[**2.2 PHYSICAL TOPOLOGY:** 7](#_Toc168267853)

[**2.3 FOURIER TRANSFORM:** 8](#_Toc168267854)

[**2.4 FOURIER TRANSFORM APPLICATIONS USED IN THE TOPOLOGY:** 9](#_Toc168267855)

[**2.5 DATA TRANSMISSION BETWEEN DEVICES:** 10](#_Toc168267856)

[**2.5.1 SAMPLING:** 10](#_Toc168267857)

[**2.5.2 QUANTIZATION:** 11](#_Toc168267858)

[**2.5.3 MODULATION:** 11](#_Toc168267859)

[**2.5.4 DEMODULATION:** 11](#_Toc168267860)

[**2.6 IMPAIRMENTS OF THE SIGNAL:** 12](#_Toc168267861)

[**2.6.1 NOISE:** 12](#_Toc168267862)

[**2.6.2 ATTENUATION:** 12](#_Toc168267863)

[**2.6.3 DELAY:** 12](#_Toc168267864)

[**2.6.4 JITTER:** 13](#_Toc168267865)

[**2.6.5 INTERFERANCE:** 13](#_Toc168267866)

[**2.7 BPDU:** 13](#_Toc168267867)

[**2.8 SPANNING TREE PROTOCOL:** 14](#_Toc168267868)

[**2.8.1 CONVERGENCE OF STP:** 14](#_Toc168267869)

[**2.8.2 RECONVERGENCE OF STP:** 14](#_Toc168267870)

[**2.8.3 ALTERNATIVES OF STP:** 15](#_Toc168267871)

[**2.9 PEER TO PEER PROTOCOL** 15](#_Toc168267872)

[**2.9.1 ADVANTAGES** 15](#_Toc168267873)

[**2.9.2 DISADVANTAGES** 15](#_Toc168267874)

[**2.10 INTER-VLAN ROUTING:** 16](#_Toc168267875)

[**CHAPTER 3** 17](#_Toc168267876)

[**3.1 DEVICE CONFIGURATION:** 17](#_Toc168267877)

[**3.2 TEST PLAN:** 38](#_Toc168267878)

[CHAPTER 4 48](#_Toc168267879)

[**4.1 CONCLUSION:** 48](#_Toc168267880)

# **EXECTIVE SUMMARY**

The Atlantic Connectify Solutions, a technology solutions provider consists of approximately 50 to 60 employees, requires an efficient network infrastructure to support its operations. The company needs a seamless layer 1 infrastructure with wired connectivity using Ethernet cabling, along with layer 2 network involving VLAN implementation and Ethernet switches for effective communication and network management. The network design includes connecting nearly 50 workstations and 3 high-performance servers using Ethernet cables to ensure high performance and efficiency. The company consists of four departments (Management, Development, Delivery, and Client) each have separate VLANs to segregate network traffic and improve security and manageability.

To meet these requirements, a comprehensive network topology was created with four VLANs assigned to the respective departments. Inter-VLAN routing was enabled to facilitate communication between VLANs, ensuring seamless connectivity across the organization. The network's performance and configuration were verified using the Cisco Packet Tracer simulation tool, where successful ping responses between PCs and servers across different VLANs and confirmed the network's reliability and efficiency. This infrastructure will support Atlantic Connectify Solutions' IT management, software development, data center migration, and data security operations, helps to deliver technology solutions to their clients effectively.

# **CHAPTER 1**

## **1.1 COMPANY OVERVIEW:**

Atlantic Connectify Solutions is service based company consists around 50 to 60 employees who delivers technology related solutions to their clients. They take projects from the client and understand their need and then provide the proper solutions to them which includes managing the IT infrastructure, development of custom software based on their needs, migration of data centers from on premise to cloud platforms, implement and maintain security of the data etc.…. The company consists of many departments like development, management, delivery and so on.

## **1.2 NETWORK REQUIREMENTS:**

The Atlantic Connectify Solutions requires a seamless layer 1 infrastructure with wired connectivity using ethernet cabling additionally, layer 2 network crucial involving the implementation of VLANs and ethernet switches to facilitate efficient communication and network management. The computing need include high performance servers and workstations. The company consists of nearly 50 computers and 3 servers. All the PC’s and servers need to be connected with wired connections with ethernet cables and the network needs high performance and efficiency. Then the four departments (Management, Development, Delivery and Client). The management team consists of 15 workstations and 3 servers, Development team consists of 20 workstations and the delivery team has around 15 PC’s and these four departments need to be separated by using the VLAN’s as a layer 2 requirement. Then there should be a communication between every VLAN (i.e. management, delivery, development and client).

# **CHAPTER 2**

## **2.1 LOGICAL TOPOLOGY:**

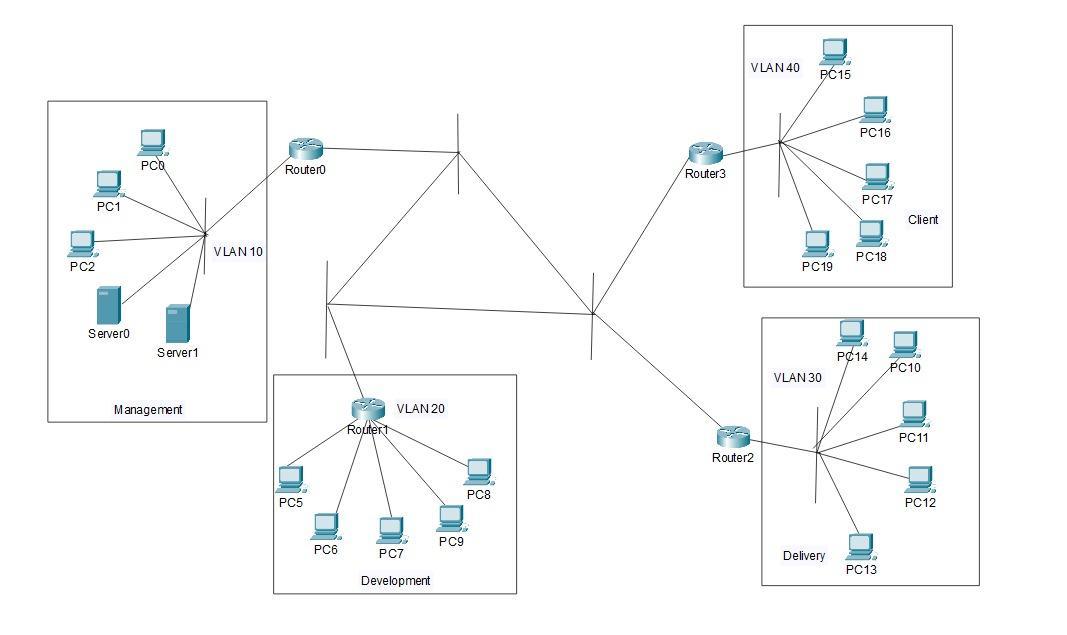


Figure 2.1 Logical Topology

## **2.2 PHYSICAL TOPOLOGY:**

The physical topology consists of seven switches, 4 routers, 18 PC’s and 2 servers all are interconnected with each other and four departments (Management, Development, Delivery and Client) in the company is assigned to separate VLAN’s named VLAN 50, VLAN 20, VLAN 30, VLAN 40 respectively. Each VLAN has 5 PC’s needs to be interconnected.

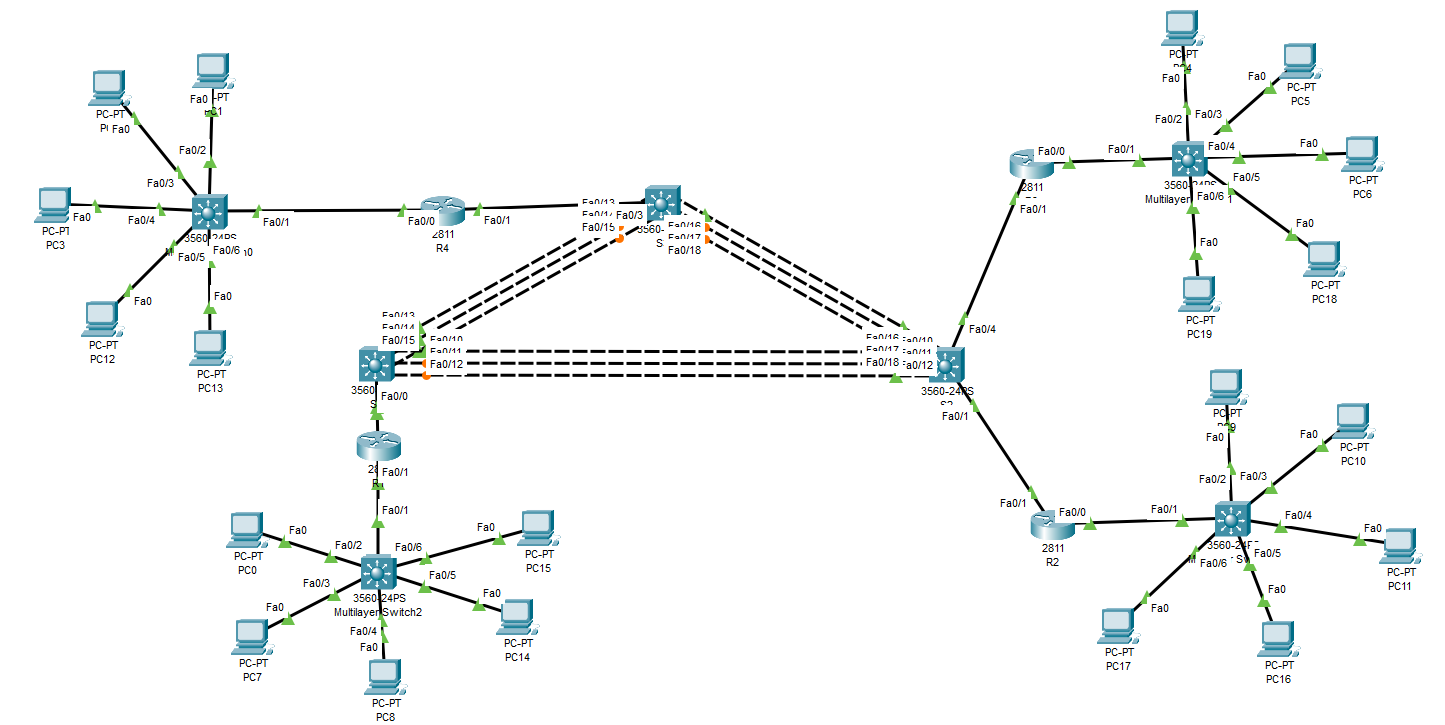


Figure 2.2 Physical Topology

## **2.3 FOURIER TRANSFORM:**

In General Fourier transform is the mathematical technique which is used to convert the signal which is in time domain into the signal in frequency domain.

Based on the physical topology the data transferred between the devices like PC and Switches are in the form of signals which consists of unwanted noise at certain frequencies and due to this the output may affected and the reliability of the data transmission decreases. In such cases by applying the Fourier transform the signal’s frequency component has been analysed and the unwanted noise and some impairments has been identified and filtered out which makes the improvement in signal to noise ratio and the reliability of the transmission is increased and after filtering the noise from the signal in frequency domain and then to convert it back to the time domain, inverse Fourier transform is used.

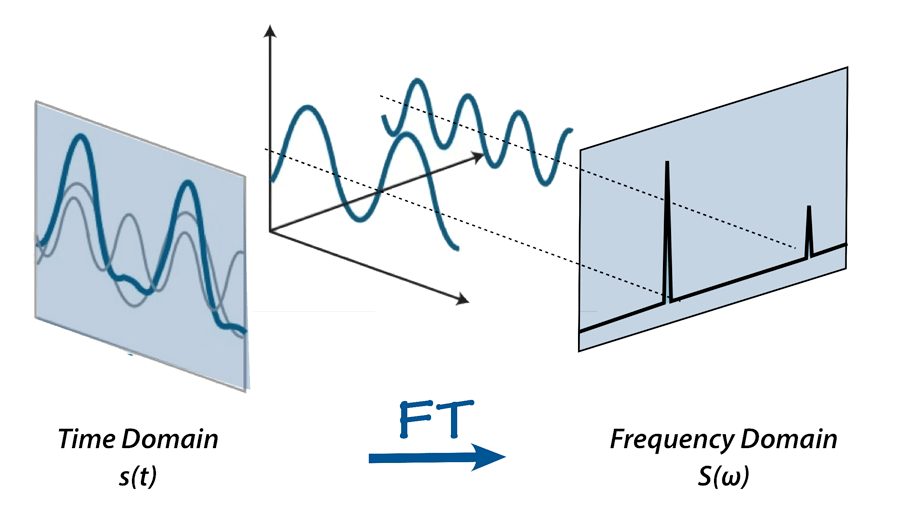


Figure 1.3 Fourier Transform (Time domain to Frequency domain)

Usually the communication between the PC, Switch and server is in the form of signals in modern communication most of data transmission in digital signals. In this topology let’s take a communication between a PC and a switch as an example. Before transmission, data generated on a PC typically exists as digital signals. The Fourier Transform can analyze and represent these digital signals in the frequency domain. Subsequently, the digital signal is converted to analog form for transmission. As it travels through the transmission channel, it may encounter impairments like attenuation and distortion, resulting in noise. At the receiving end, sampling occurs the process to convert the analog signal to digital signal, this involves taking samples of the analog signal to retrieve the original data sent by the sender. Each sample's height is then determined and adjusted into levels through quantization. This process ensures that the samples match predefined levels. Quantization is irreversible; once applied, it cannot be undone. Following quantization, filters are utilized to eliminate impairments. Finally, the analog signal is converted back into digital form, allowing the original data to be retrieved at the receiver end if the receiver end is server or a database in order to store the data we use the same digital format.

## **2.4 FOURIER TRANSFORM APPLICATIONS USED IN THE TOPOLOGY:**

**Signal Processing and Noise reduction:**

Computer networks use various media (cables, wireless, etc.) to send signals carrying data. The quality of data transmission may suffer due to noise and interference caused by these signals.

The Fourier Transform can be used to examine a signal's frequency components. The signal-to-noise ratio can be increased and data transmission reliability increased by identifying and filtering out unwanted noise, which is usually present at specific frequencies.   
Signal reconstruction involves converting the signal back to the time domain using the Inverse Fourier Transform after eliminating noise in the frequency domain to guarantee the accuracy of the data obtained.

**Analyzing Network Performance**

There are several aspects of network performance, such as packet loss, latency, and bandwidth usage, is necessary for analysis.

Bandwidth Utilization:

Using the frequency domain to convert network traffic data, managers may see how bandwidth is being used, find inefficiencies, and optimize bandwidth allocation.   
Studying the frequency components of time-series data from packet transfers allows the analysis of latency and jitter. This aids in locating irregularities or recurring delays that could impair network performance.

**Implementation of Fourier transform in network devices:**

Fourier transform is used by switches and routers to optimize routing methods and assess signal integrity. Additionally, they use it in quality of service (QoS) measures to efficiently prioritize and control traffic using real-time data.

Tools for Network Monitoring:

The Fourier Transform is used by tools and software intended for network monitoring to examine traffic patterns, spot irregularities, and offer comprehensive data on the functionality and health of network.

PCs and servers:

Fourier transform is useful for these endpoints in applications that deal with resource allocation, performance diagnostics, and local network optimization. It also ensures effective operation and connectivity.

## **2.5 DATA TRANSMISSION BETWEEN DEVICES:**

When the data is transmitted from one device to another device there are several fundamental processes happens, they are Sampling, Quantisation, Modulation, Demodulation, Filtering.

### **2.5.1 SAMPLING:**

Initially the data from one device to another device is transferred in the form of signal. Let us take a communication between a PC and a switch and consider PC as sender and switch as receiver the data first generated inside the PC is in the form of digital signal and then it needs to be converted to analog signal to transfer it through the cable for this signal conversion the first and initial step is known as sampling in which the samples of the signal are taken in the regular intervals from the original signal and then with the help of the samples the digital signal is converted into analog signal. The number of samples must satisfy the sampling theorem (number of samples = 2 times the Nyquist rate). If it is lesser, it undergoes aliasing else if it increases it leads an irregular signal as an output.

### **2.5.2 QUANTIZATION:**

The technique of mapping a signal's continuous amplitude values to a limited number of discrete levels is known as quantization, and it is used in signal processing and data compression. For effective data storage and transfer in digital systems, this analog to digital conversion is necessary. The process of quantization involves sampling the data at regular intervals and truncating or rounding each sample to the closest value in the quantization levels. The number of quantization levels, or resolution, has an effect on the fidelity of the reconstructed signal. Although it demands more storage capacity, higher resolution—achieved through increasing bit depth reduces quantization error. Many digital technologies, such as digital signal processing, analog-to-digital conversion in communication networks, and compression of audio and images, depend on quantization.

### **2.5.3 MODULATION:**

The modulation happens on the sender side that is PC we considered PC as a source and a router as a destination, in modulation when the data is transmitted through the channel there must a need in modification of the signal to reach the destination properly these modifications include Amplitude modulation, Frequency modulation and Phase modulation in order to transmit the data over the channel efficiently.

### **2.5.4 DEMODULATION:**

Demodulation happens on the receiving end that is router, demodulation is the process of separating the original information signal from a modulated carrier signal. It is the modulation process in reverse and is necessary to reliably recover the original data which is transferred from the sender PC.

## **2.6 IMPAIRMENTS OF THE SIGNAL:**

### **2.6.1 NOISE:**

At the time of data transmission between the two devices like PC and Switch or Router, some interruption or disturbance that compromises the integrity and quality of the data being conveyed is known as noise between data transmission in PCs and routers. This may cause the network to have reduced speeds, higher latency, and higher error rates. Electromagnetic interference (EMI) from electronics and appliances in the home, radio frequency interference (RFI) from other wireless networks and devices that reduce signal strength are common causes of noise. Transmission noise is also caused by signal attenuation over long distances and crosstalk between cables, which can result in data packet loss and retransmissions. This can be reduced by using the cables of shorter length and high-speed connection.

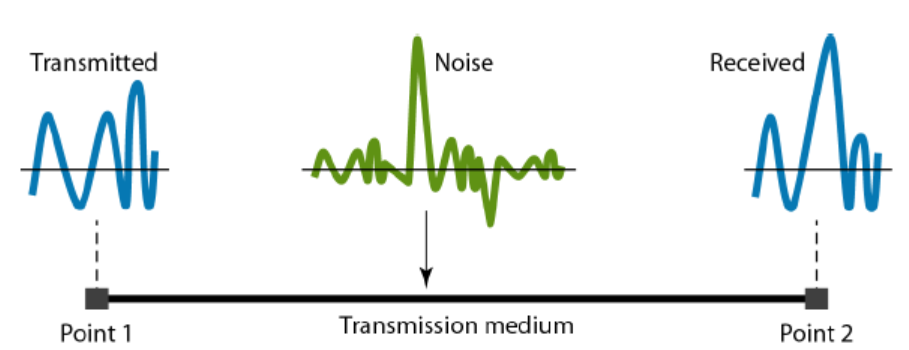


Figure 2.4 Signal with noise at receiver side

### **2.6.2 ATTENUATION:**

In the physical topology at the time of data transmitted from PC to router or switch through the wireless or wired medium like ethernet cable there is some gradual decrease in signal strength which makes the signal weaker is known as attenuation. Reduced signal strength from this weakening may cause slower data transmission rates, higher error rates, and possibly even the loss of connectivity.

### **2.6.3 DELAY:**

Delay is the term in which the time of data transmitted from the source to the destination. I our topology each device is connected with copper cables since its is a wired connection topology. Initially the sender starts the data transmission and time took by the signal to travel through the medium and it reaches the sender is the propagation delay. From the sender PC it needs to send all the data packets to the wired medium is known as transmission delay. This delay will reduce the performance of the network and it caused by the distance between the sender and receiver. This can be eliminated by reducing the distance between the source and destination, using higher bandwidth connections, Optimizing the packet size etc.. .

### **2.6.4 JITTER:**

At the time of signal transmitted through the medium there should be a jitter which is the difference in the time it takes for data packets to get from their source to their destination is referred to as jitter. Jitter is a measure of the variability of packet delays over time, as opposed to latency, which is an average delay. A number of things, including as network congestion, which causes data packets to be queued and delayed while they wait to be transmitted, and we configured with more than one routes which may leads the variation packet arrival time then the jitter occurs cause jitter. It will also be caused if the PC’s, switches and routers are not maintained in good condition.

### **2.6.5 INTERFERANCE:**

When the signal is transmitted from one PC to another PC through the wired medium in this network topology there will be some other signal will overlap with the original signal which results that the receiver will get the output signal will some changes leads an error in the output. Usually this happens mostly on switches. For eliminating this issue some protocols were used, one of the protocols mainly used is STP (Spanning Tree Protocol) which helps to eliminate the interference by keeping one port as active and it blocks the rest of the ports to the same path by considering the cost of the path which reduces the collision and interference of signal. By using this network performance and reliability is increased.

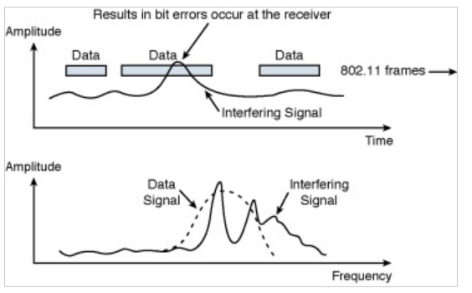


Figure 2.5 Interference of signal

### **2.7 BPDU:**

Bridge Protocol Data Unit is the packet frame which helps the switches to enable STP(Spanning Tree Protocol) by collecting the information about each bridge in our topology. It prevents the looping of data frames transmitted through multiple paths. Configuration BPDUs are generated by the Root Bridge (root switch) and spread outwards from it. The Root Bridge is identified as the switch with the lowest switch ID. The process begins by comparing switches. When a network switch receives a configuration BPDU with a lower root switch ID than the current lowest root switch ID in the network, it automatically selects the switch with the lowest root switch ID as the Root Bridge. In this process, you might wonder what role the non-root switches play. Non-root switches do not generate any configuration BPDUs. Instead, non-root switches only propagate the BPDUs generated by the Root Bridge.

## **2.8 SPANNING TREE PROTOCOL:**

In our topology STP is used to keep enabled only the root port and designated and blocking the redundant ports in order to prevent the looping of the data packets in the network. For implementing STP, BPDU is the initial frame from which the switch gathers the information about the bridges available in the network.A single bridge, or switch, is designated as the network's "root bridge" in order for STP to function. To maintain a topology free of loops, all other bridges in the network must ascertain the shortest path to take in order to reach the root bridge. Only then may they disable particular links.

### **2.8.1 CONVERGENCE OF STP:**

When the Spanning tree protocol is configured in the network topology it will forward the data packets normally until changes occurs in the topology for example if any switch is added or any switch faces failure in the port, manually reconfigure the port from blocking to forwarding and vice versa this will help the network to perform seamlessly without the failure.

### **2.8.2 RECONVERGENCE OF STP:**

If a Root Bridge failure is detected, the network will elect a new Root Bridge based on the lowest bridge ID. Switches will then update their path cost calculations to the new Root Bridge. Ports will be reassigned as Root Ports (RPs), Designated Ports (DPs), or Non-Designated Ports (NDPs) according to the updated path costs. Ports that are not part of the shortest path to the Root Bridge will enter a blocking state to prevent loops. Meanwhile, ports on the shortest path will transition to a forwarding state.

### 

### **2.8.3 ALTERNATIVES OF STP:**

**Bonus 1: SHORTEST PATH BRIDGING (SPB):**

The earlier Spanning Tree Protocols, such as Multiple STP (IEEE 802.1s), Fast STP (IEEE 802.1w), and STP (IEEE 802.1D), are replaced by these techniques. These protocols prevented redundant pathways that may lead to a Layer 2 loop. In contrast, bigger Layer 2 topologies with shorter convergence times are supported by SPB, which permits all paths to be active. By permitting the utilization of every physical connection in the network, SPB provides load-sharing across all paths in a mesh network. This leads to increased efficiency and better use of the network's resources. Because SPB keeps Ethernet plug-and-play, human error in network setting is almost completely eliminated. It streamlines the configuration process, increasing accessibility and manageability of networks.

## **2.9 PEER TO PEER PROTOCOL**

### **2.9.1 ADVANTAGES**

There is no need for a central server, which lowers the possibility of a single point of failure. increases robustness and dependability since the network can keep going even when some of its peers stop working. It is easily scalable to support a big group of peers. The overall capacity and performance of the network improve with the number of peers. Peers are able to share resources including computing power, storage, and bandwidth. economical use of resources, which may result in reduced expenses for certain consumers.

### **2.9.2 DISADVANTAGES**

Peers are open to several kinds of attacks, including those that distribute malware, compromise data, or grant unwanted access. The enforcement of security policies may be difficult in the absence of central monitoring. Depending on network circumstances and peer capabilities, performance can vary greatly. Users may encounter delays and decreased performance if their connections are slower or have less bandwidth. Peer-to-peer network management and upkeep can be challenging, particularly as the network expands. obstacles in maintaining dependable and regular peer-to-peer connection. Having data stored on several peers can result in inefficiencies and redundancies. It can be difficult to synchronize and preserve data consistency amongst peers.

## **2.10 INTER-VLAN ROUTING:**

The process of deploying a router in a network to forward traffic between distinct VLANs is known as inter-VLAN routing. VLANs logically divide a switch into distinct subnets. An administrator can set up a router to redirect traffic across the multiple VLANs that are specified on the switch when the router is connected to the switch. Regardless of the VLAN set up on the switch, traffic from user nodes within the VLANs is forwarded to the router, which subsequently forwarded it to the destination network.

**BONUS 2:**

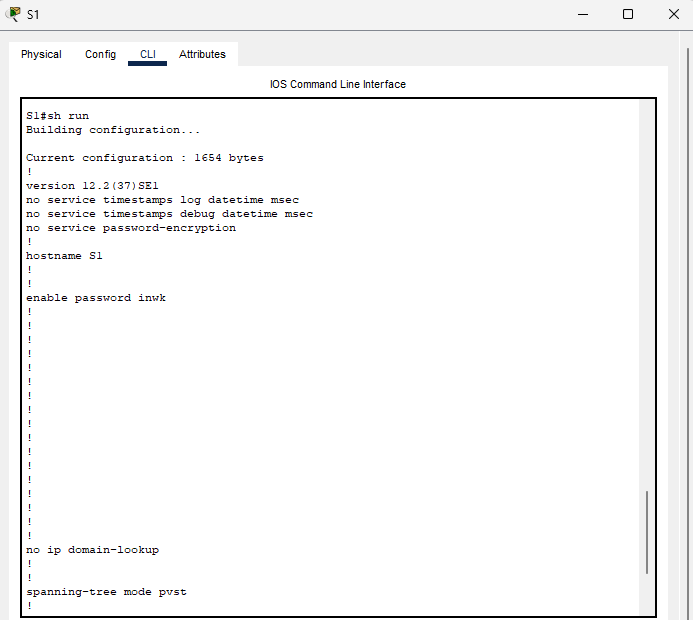
Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Protocol (PPP) are linked by means of encapsulation, wherein L2TP packets enclose PPP frames. PPP can now function across a wider range of network configurations than it has historically supported because to its encapsulation, which makes it possible for PPP data to be transferred over IP networks. The encapsulated PPP frames go through a tunnel established by the L2TP protocol over the internet or other IP-based networks, preserving the functionality and integrity of the PPP connection. PPP connections can endure and function well over long distances and over a variety of network media because to this tunneling.

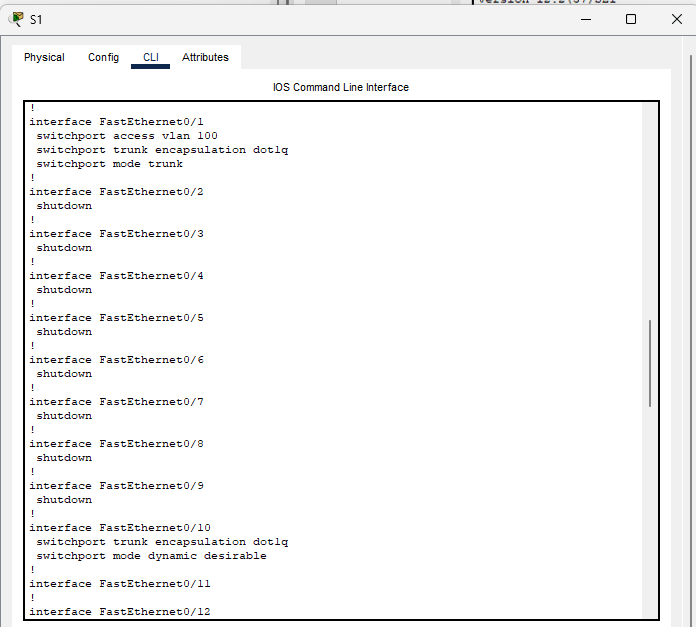
Leveraging the interaction between L2TP and PPP is important to the company working on this project since it makes scalable and secure VPN solutions possible. Combining these two elements allows for safe remote access to internal networks while supporting many protocols over a single VPN connection and offering the flexibility and scalability required to adjust to evolving business requirements. Deliverable 3 will showcase the project's potential to provide reliable, affordable network solutions that improve security and operational effectiveness, showcasing the company's capacity to offer cutting-edge and adaptable networking services.

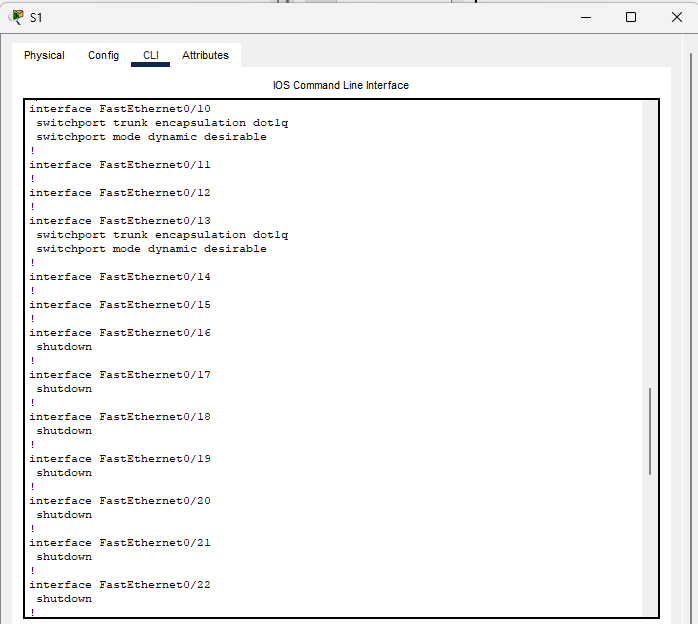
# **CHAPTER 3**

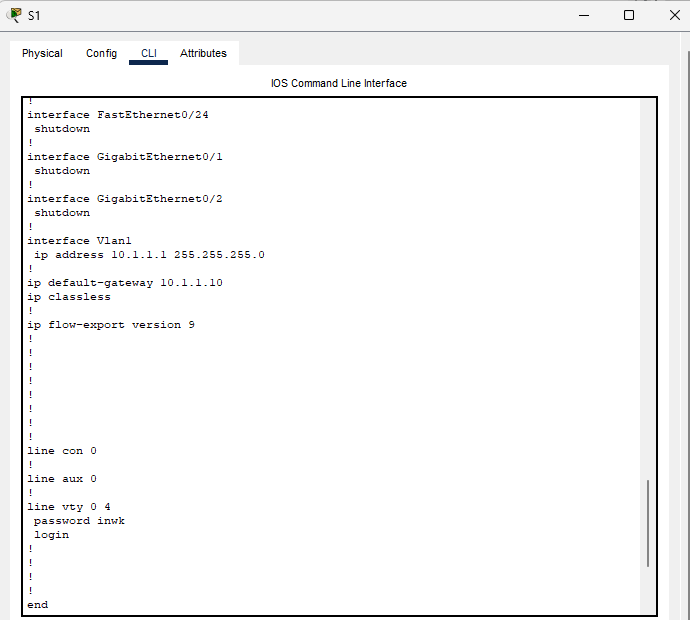
## **3.1 DEVICE CONFIGURATION:**

Running configuration of Switch S1:

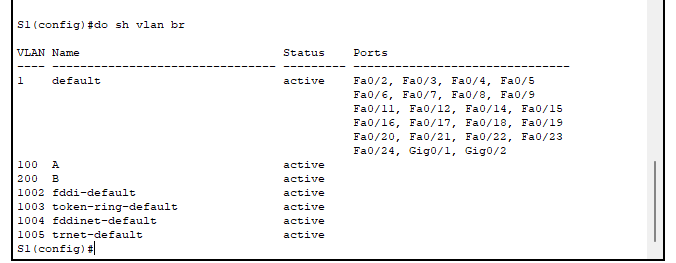




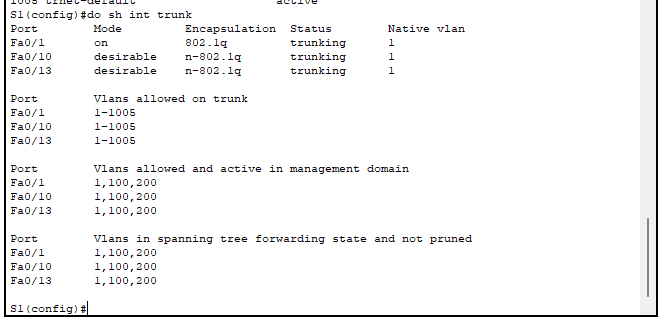




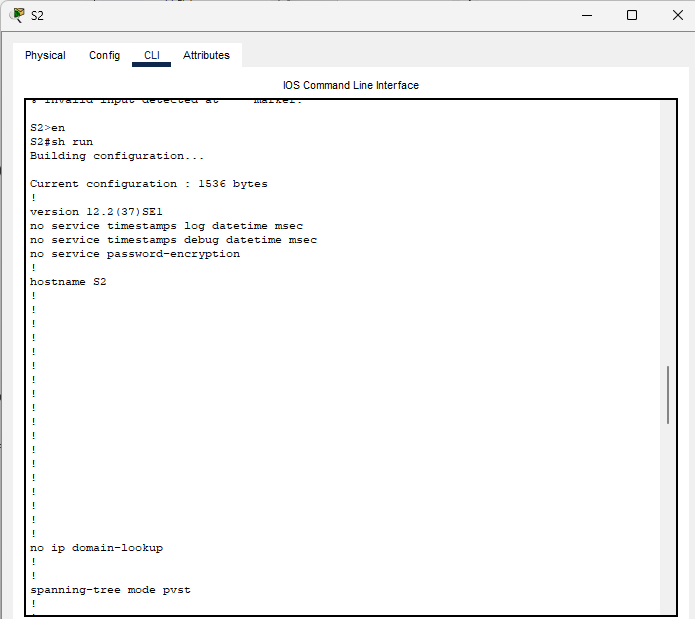
VLAN in Switch S1:

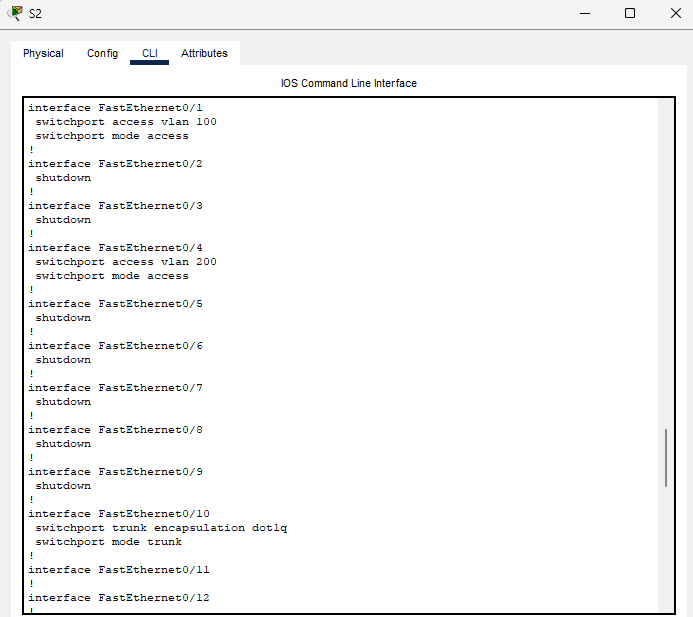


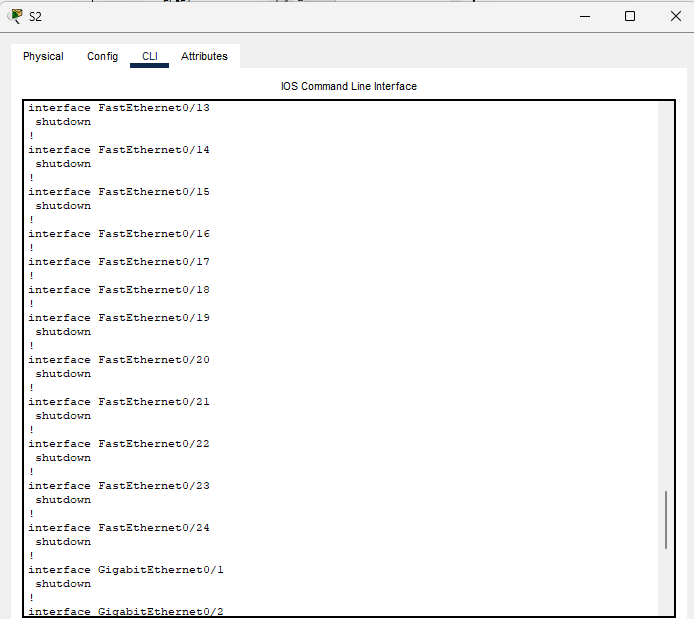
Configuration of Trunking in switch S1:

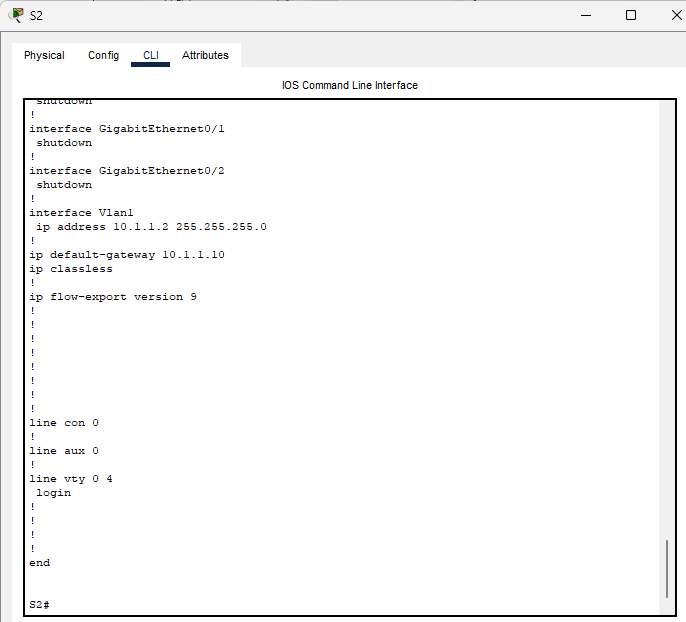


Running Configuration of Switch S2:

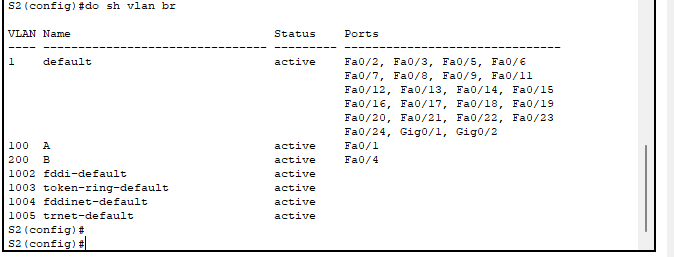


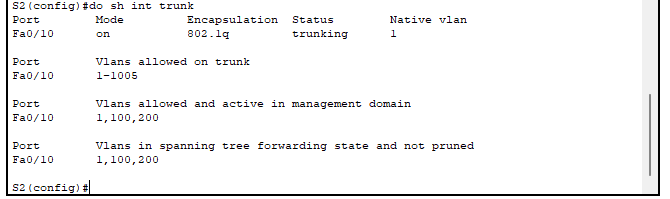




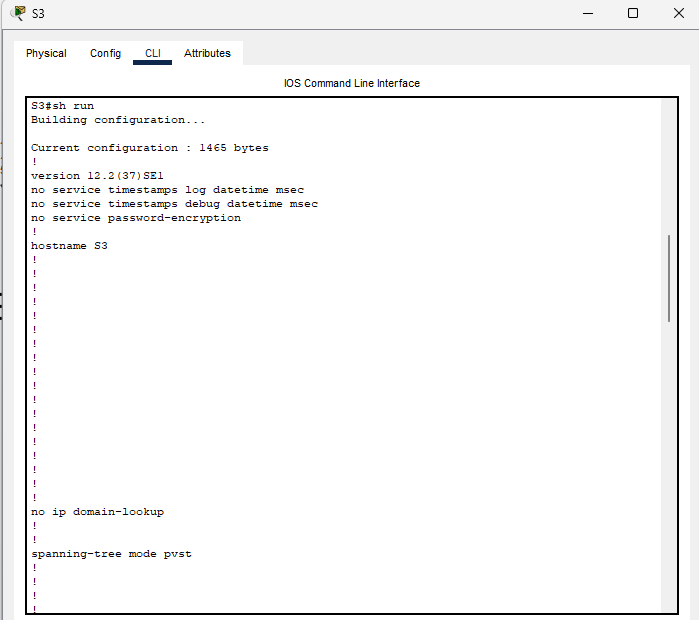


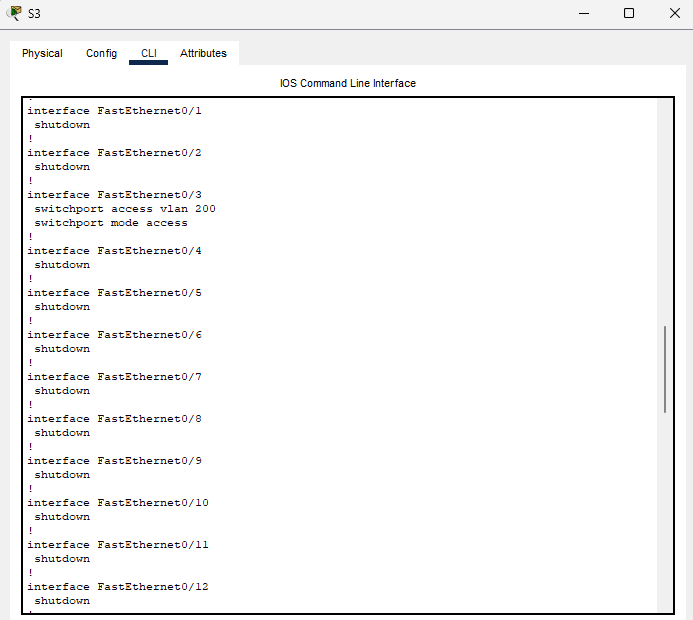
Configuration of VLAN in switch S2:

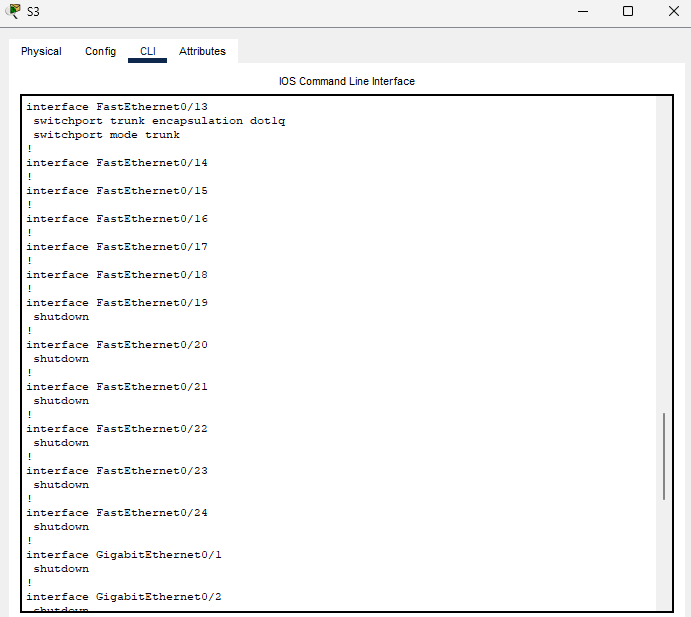


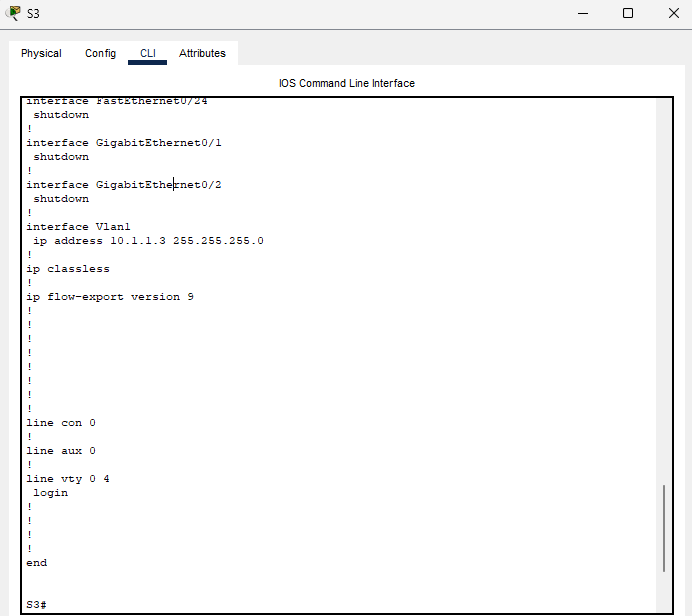
Configuration of Trunking in Switch S2: 

Running configuration of Switch S3:

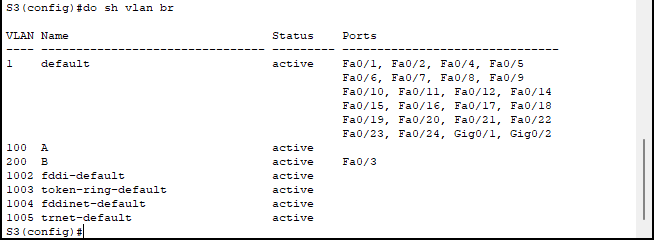




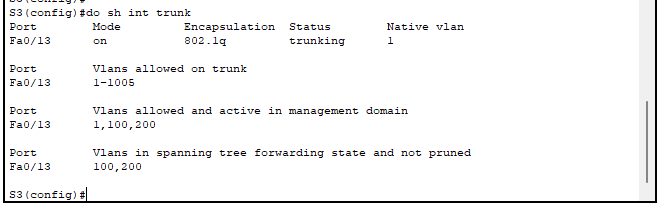




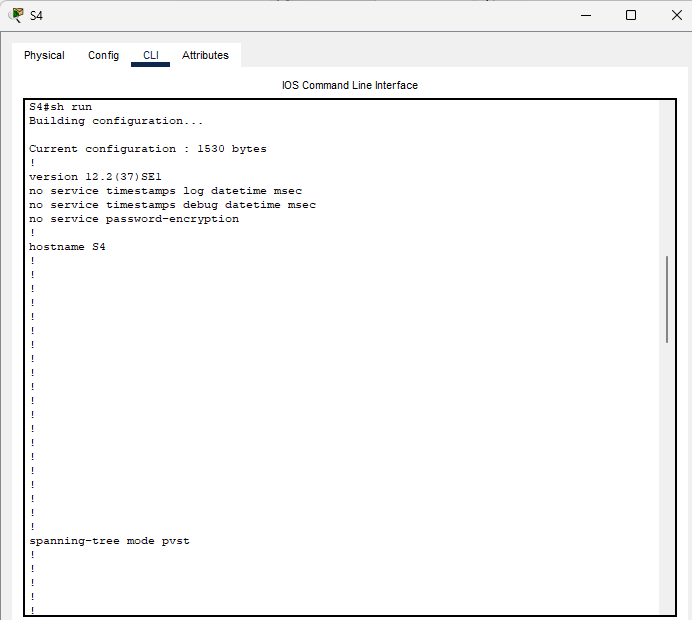
Configuration of VLAN in Switch S3:

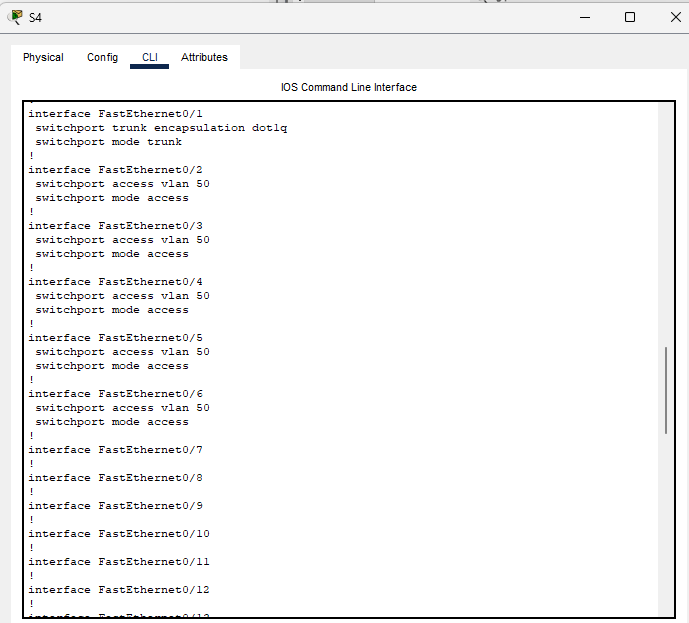


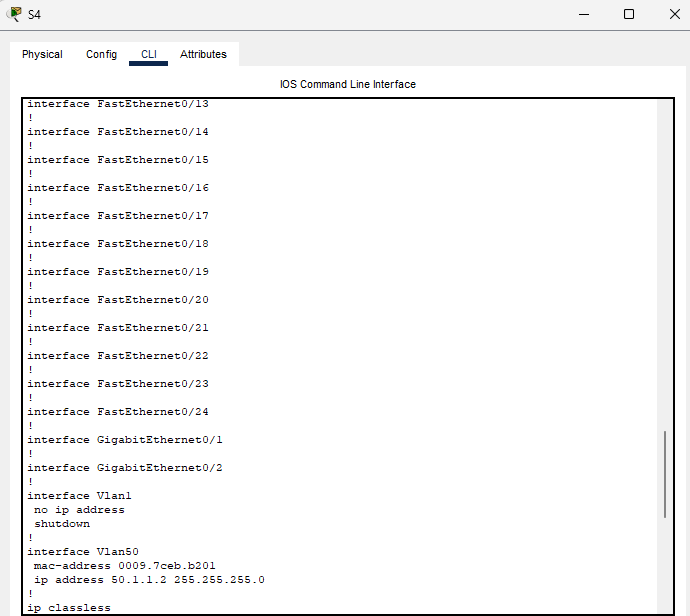
Trunking in Switch S3:

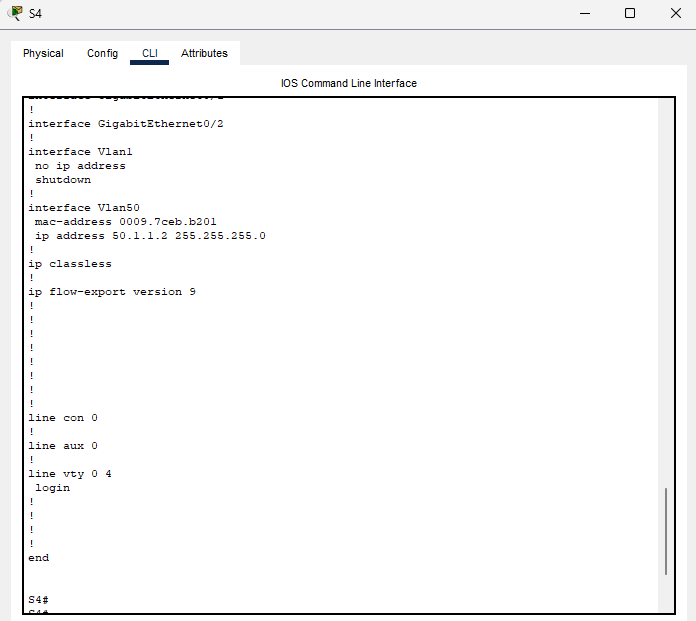


Running configuration of Switch S4:

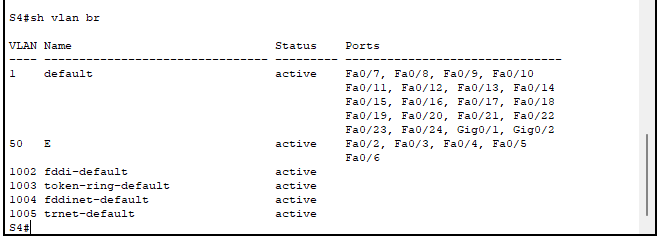




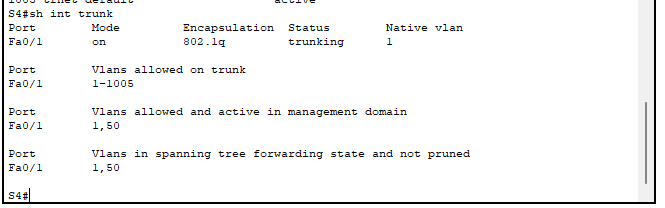




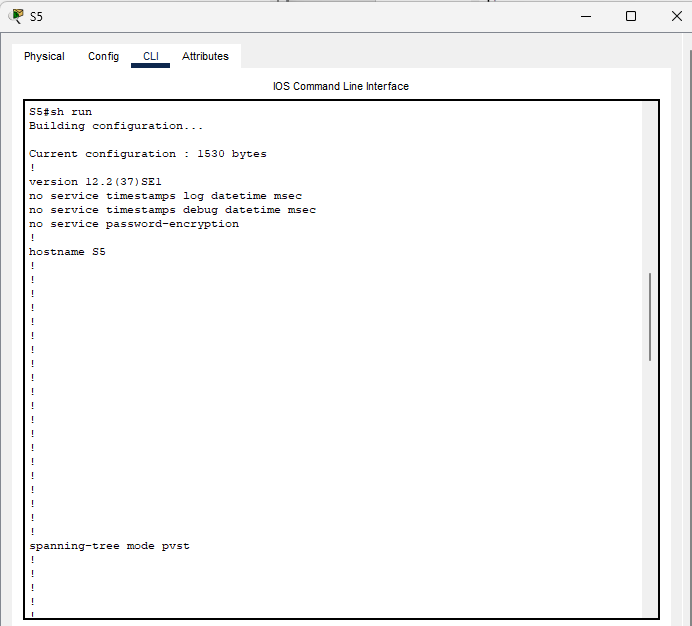
VLAN in Switch S4:

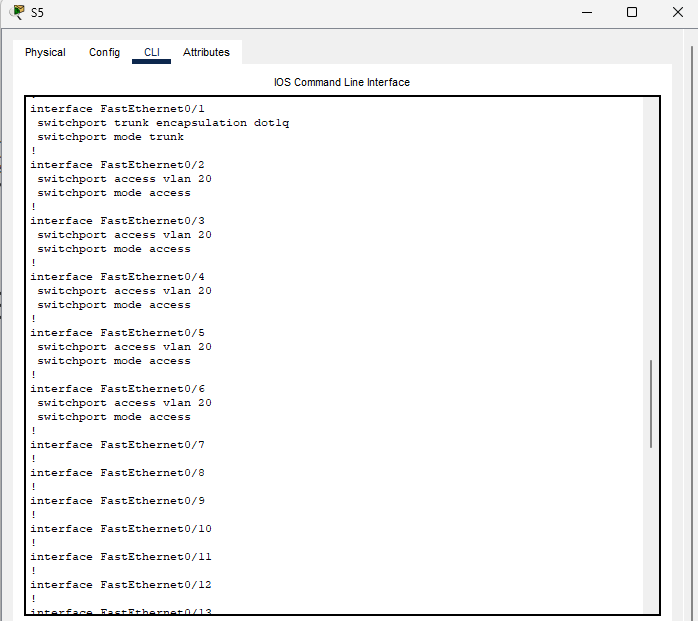


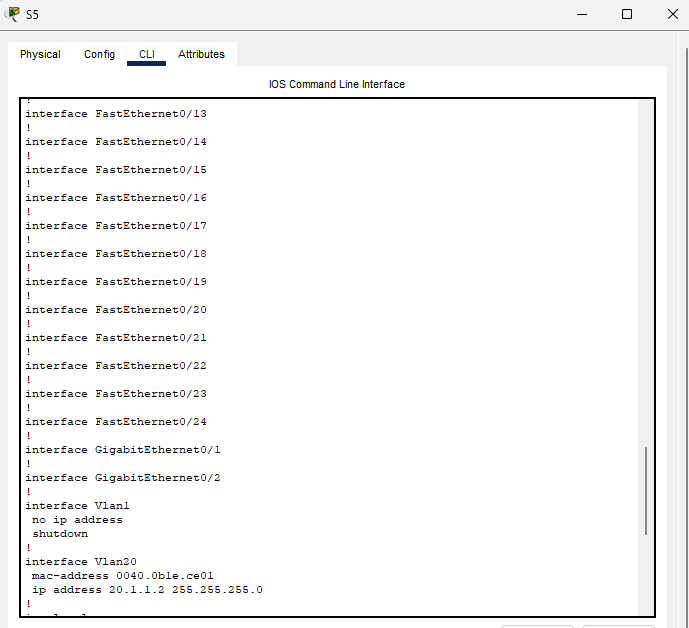
Trunking in Switch S4:

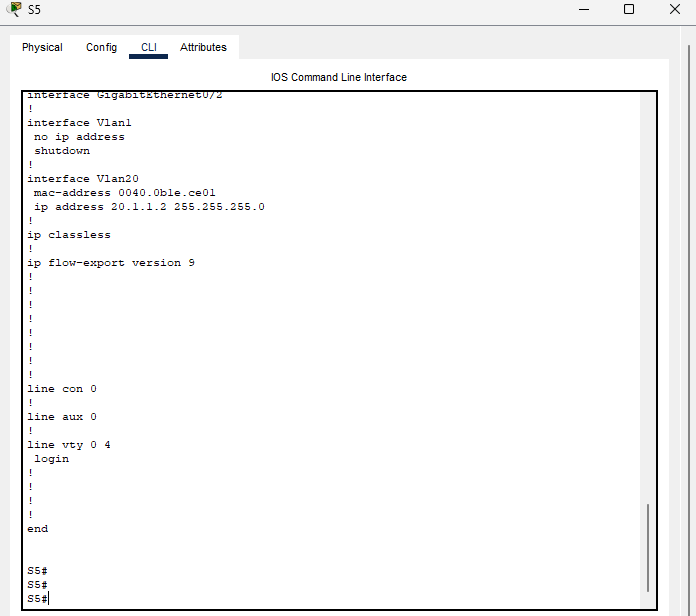


Running configuration of Switch S5:

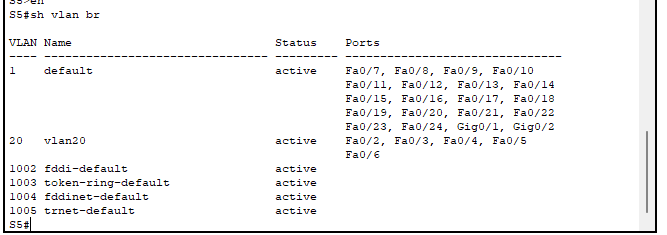




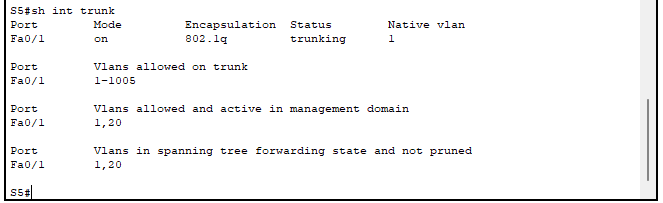




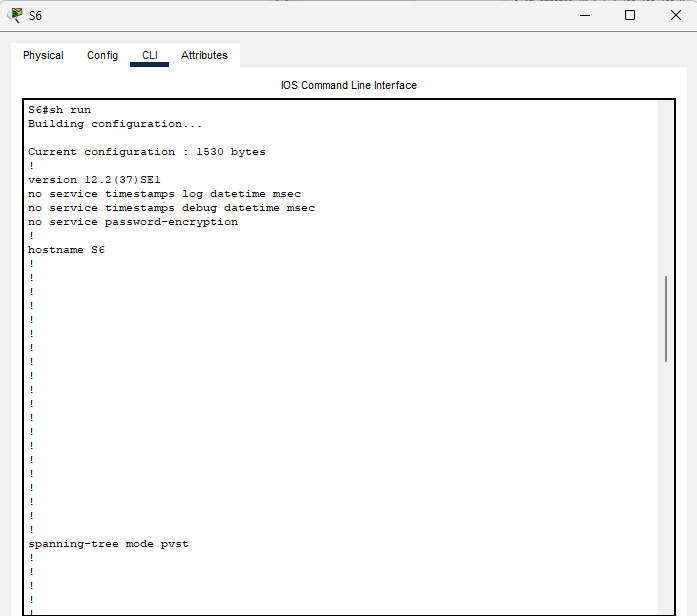
VLAN in Switch S5:

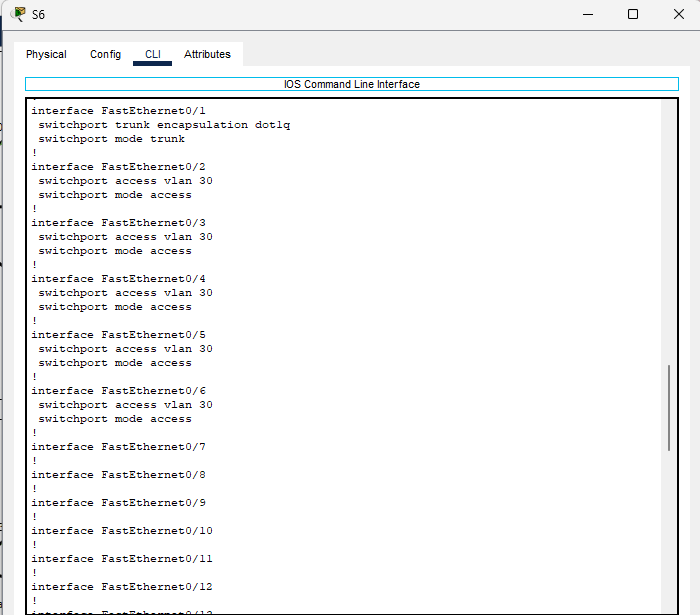


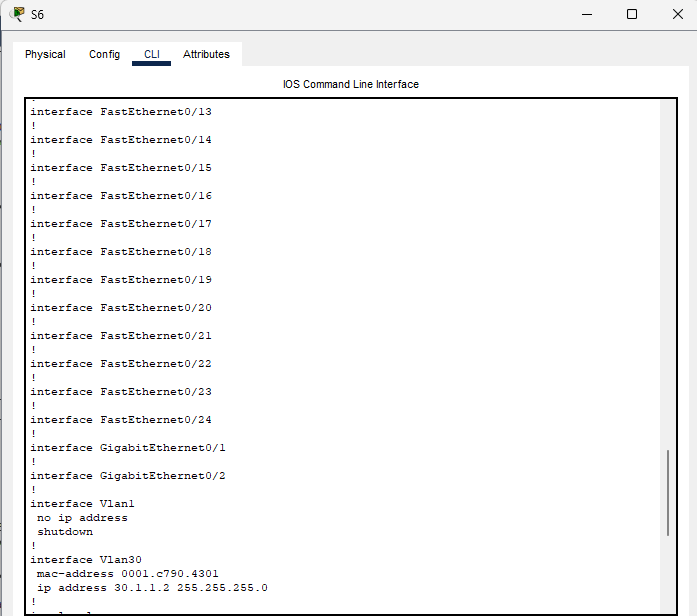
Trunking in switch S5:

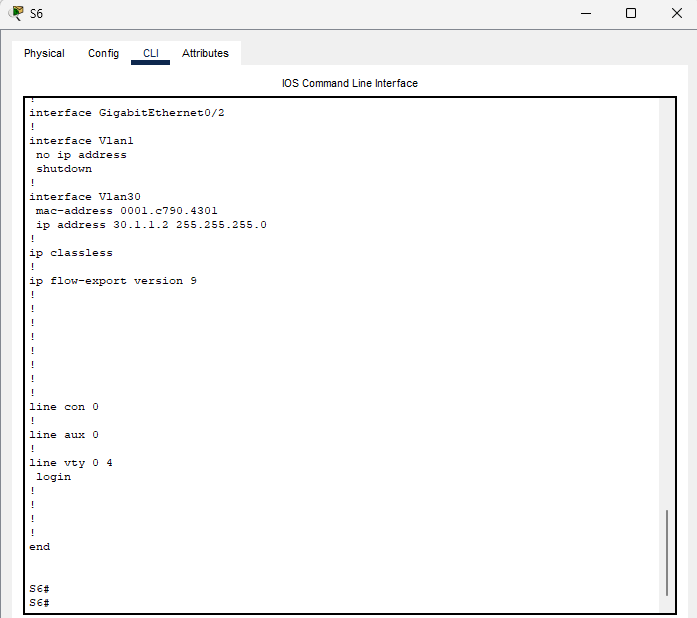


Running configuration of Switch S6:

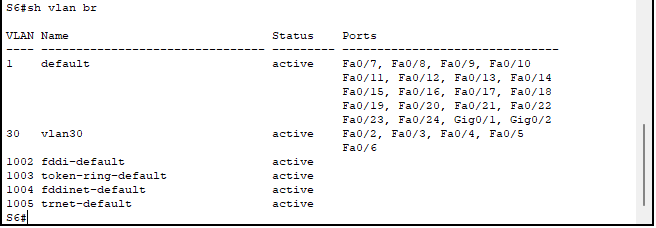




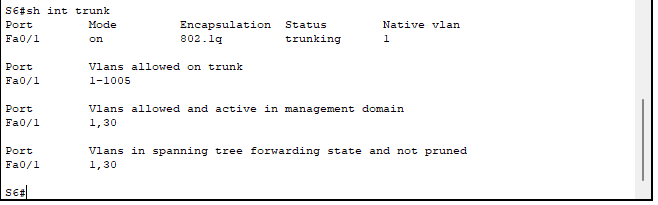




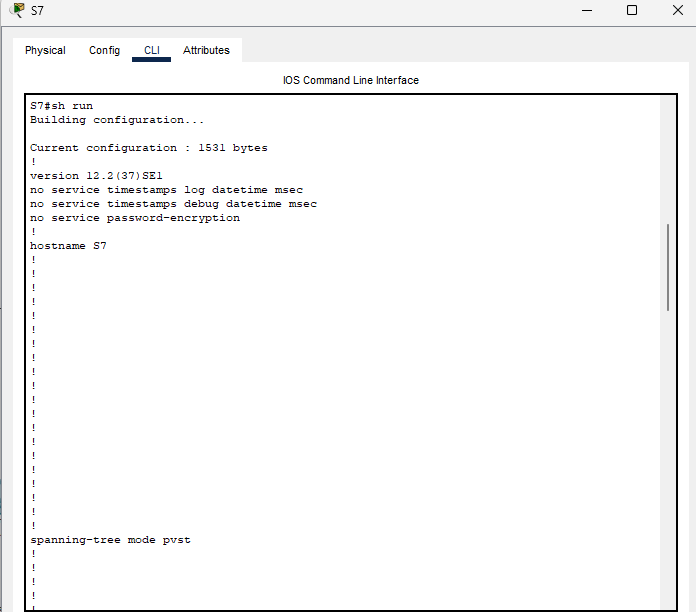
VLAN in Switch S6:

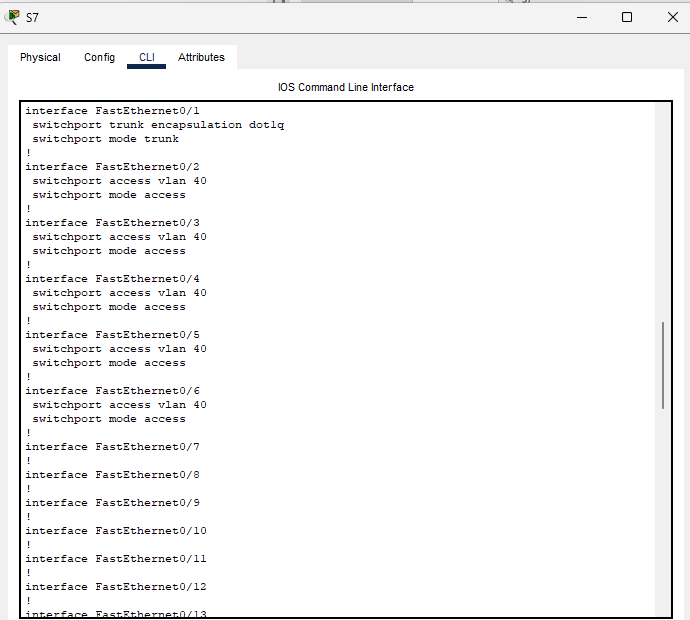


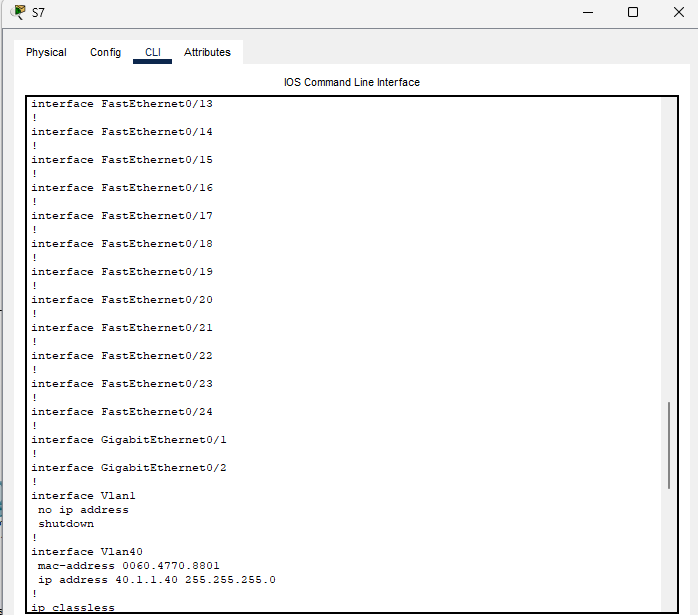
Trunking in Switch S6:

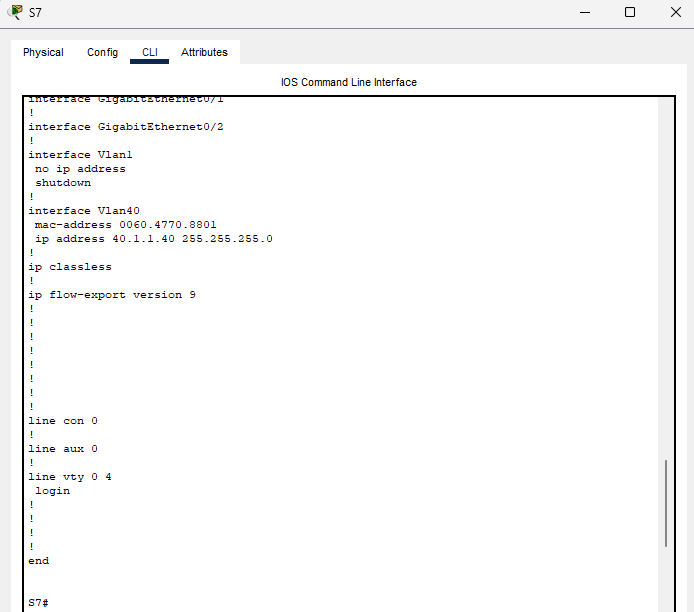


Running Configuration of Switch S7:

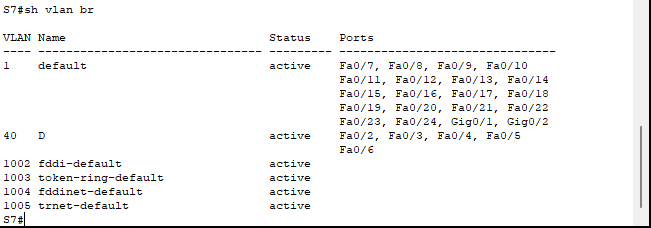




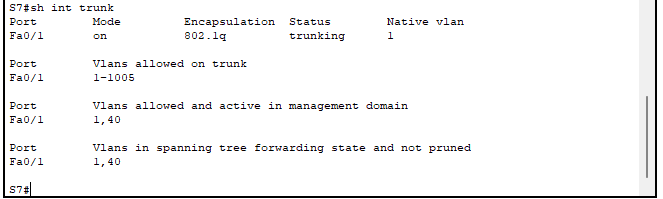




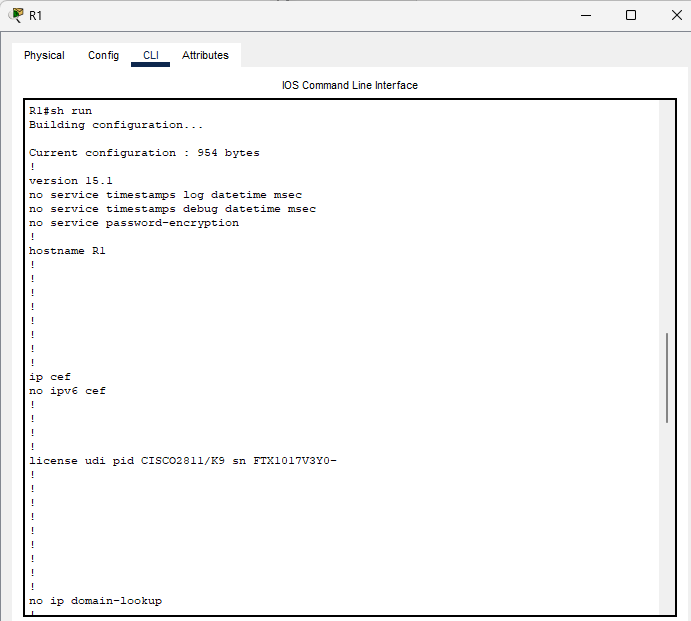
VLAN in Switch S7:

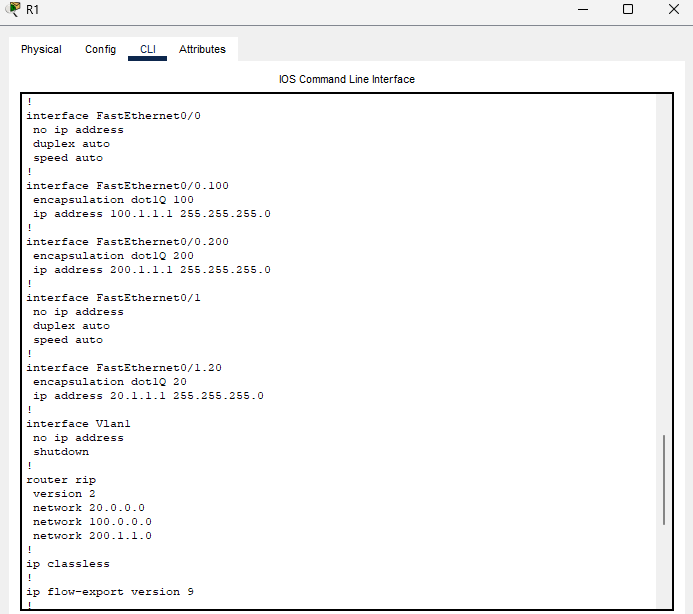


Trunking in Switch S7:

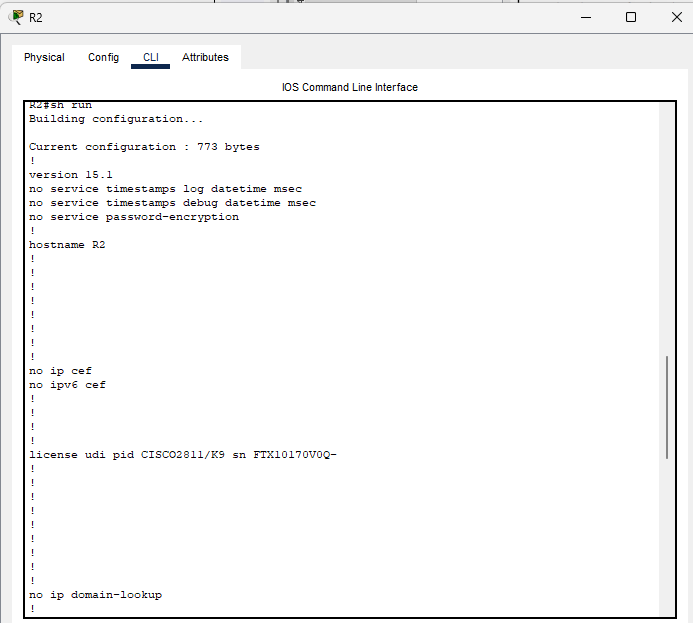


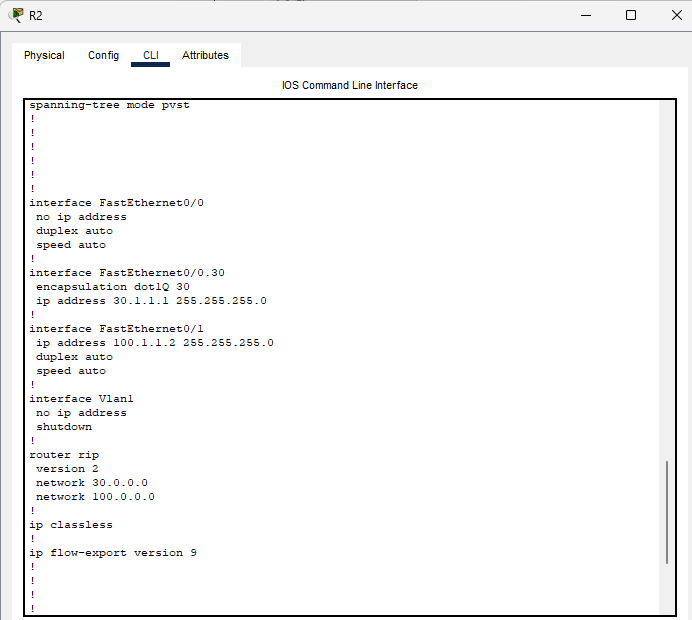
Running Configuration of Router R1:



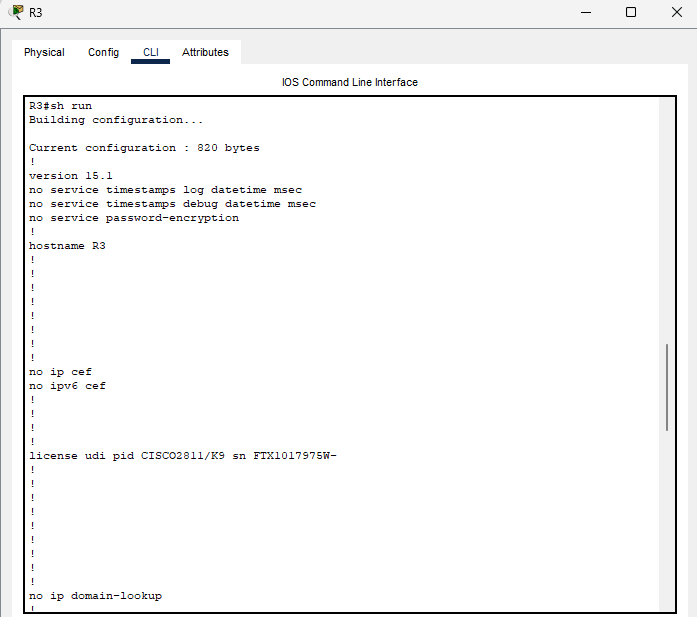


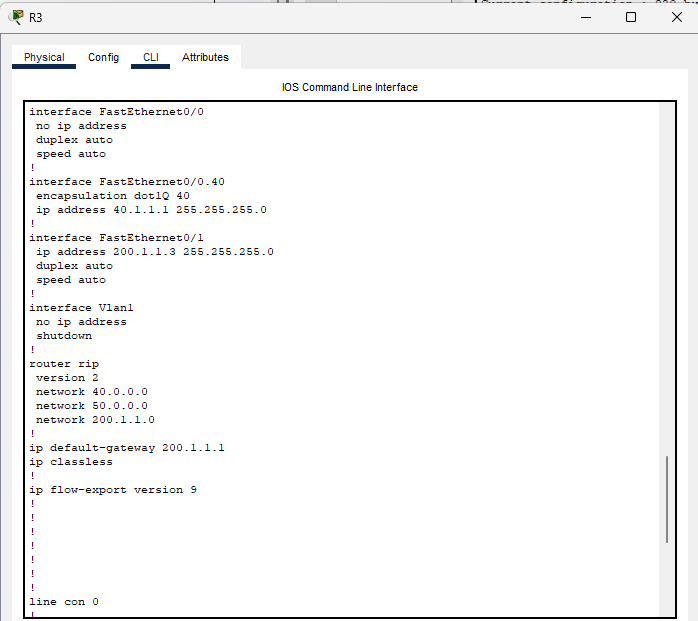
Running configuration Router R2:



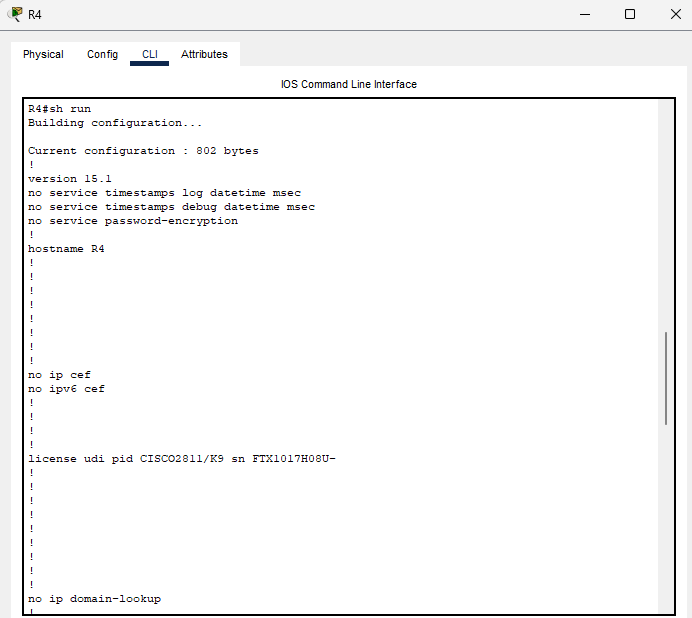


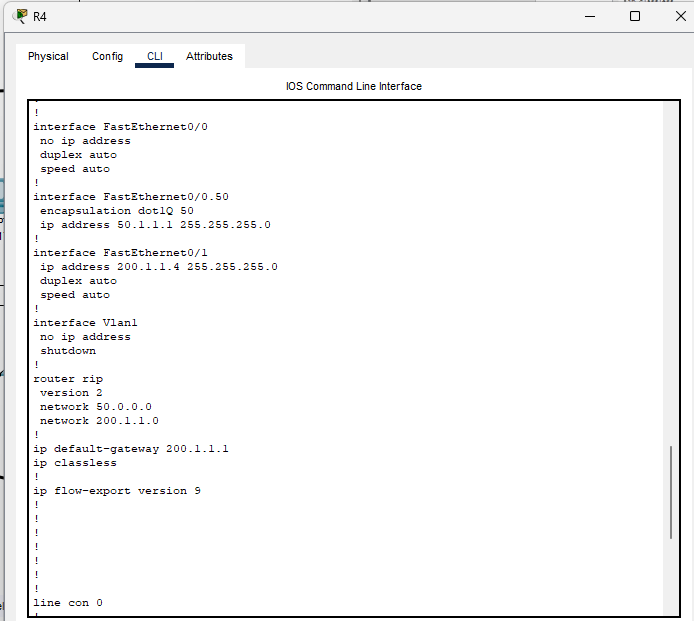
Running Configuration Router R3:





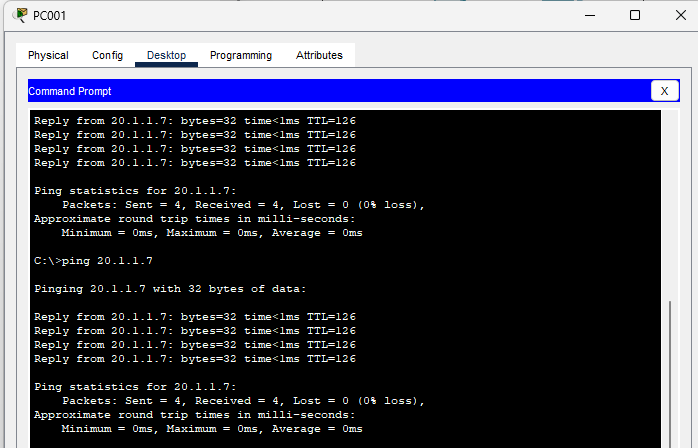
Running configuration of Router R4:



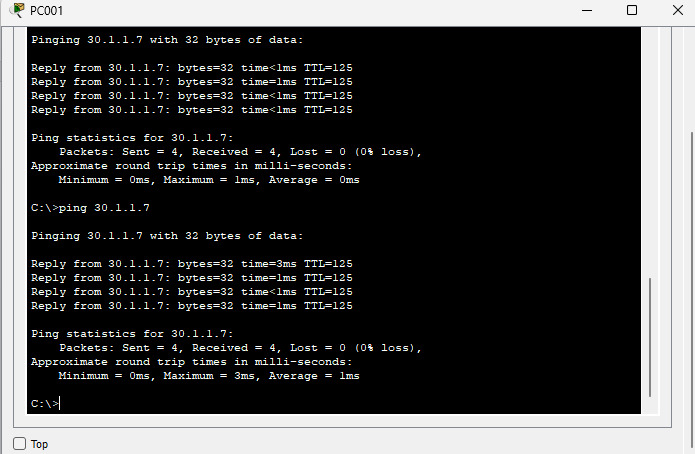


## **3.2 TEST PLAN:**

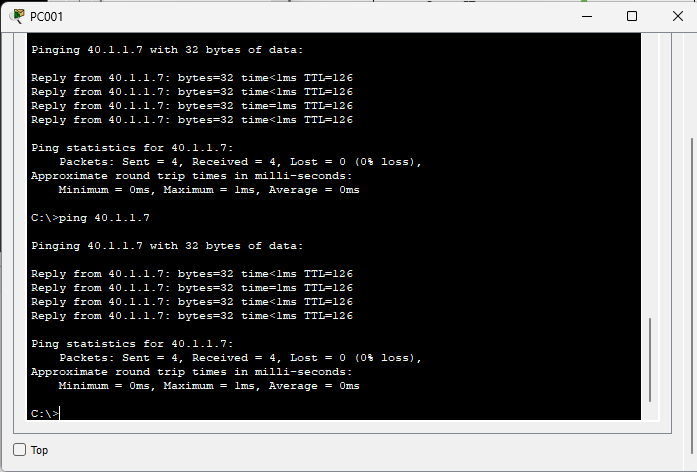
Testcase 001: When we ping from PC001(vlan 50) to PC008(vlan 20), we will get the replay successfully.



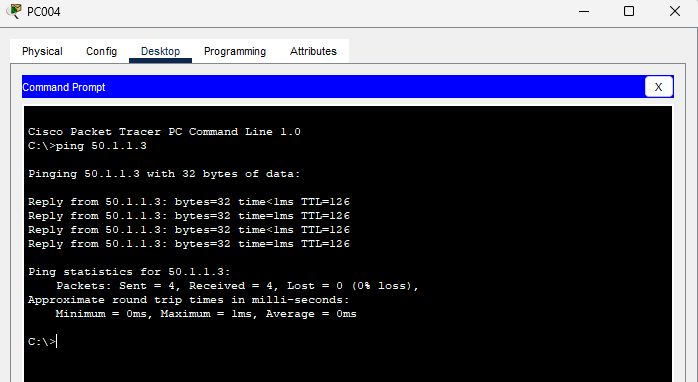
Testcase 002: When we ping from PC001(Vlan 50) to PC0013(Vlan 30),we will get the replay successfully.



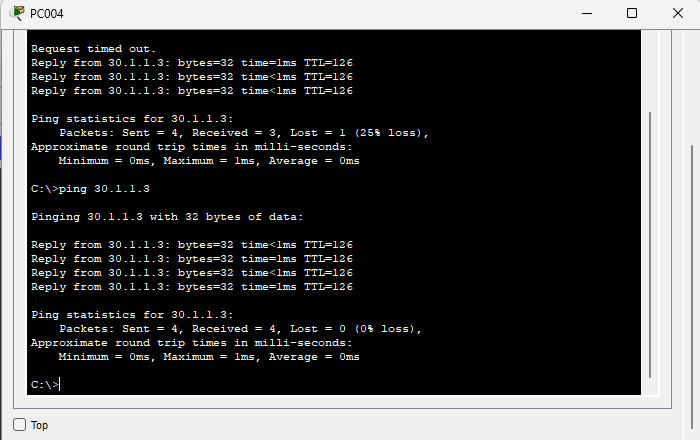
Testcase 003: When we ping from PC001(Vlan 50) to PC0018(Vlan 40), we will get the replay successfully.



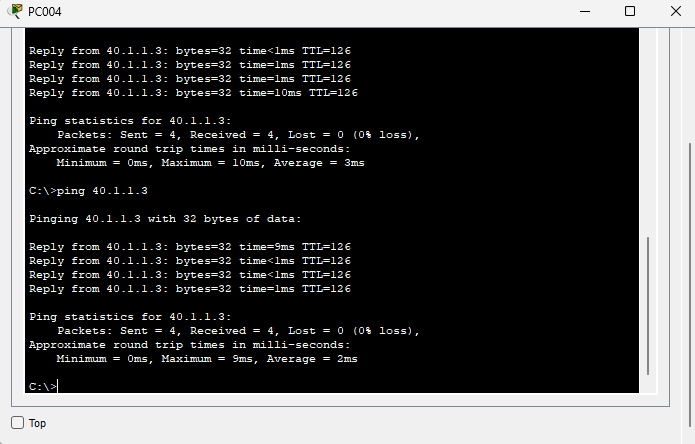
Testcase 004: When we ping from PC004(Vlan 20) to PC001(Vlan 50), we will get the replay successfully.



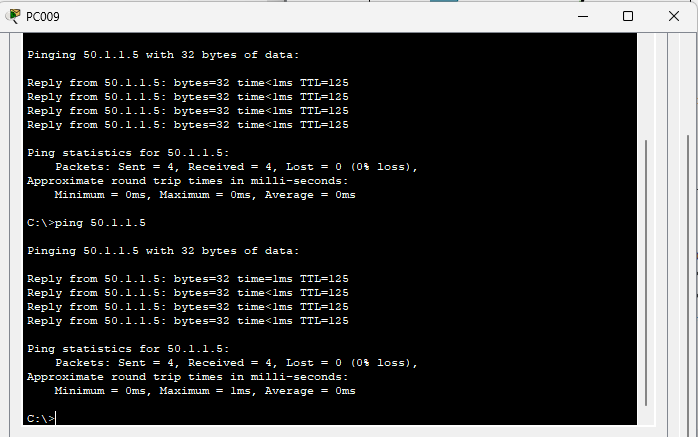
Testcase 005: When we ping from PC004(Vlan 20) to PC009(Vlan 30), we will get the replay successfully.



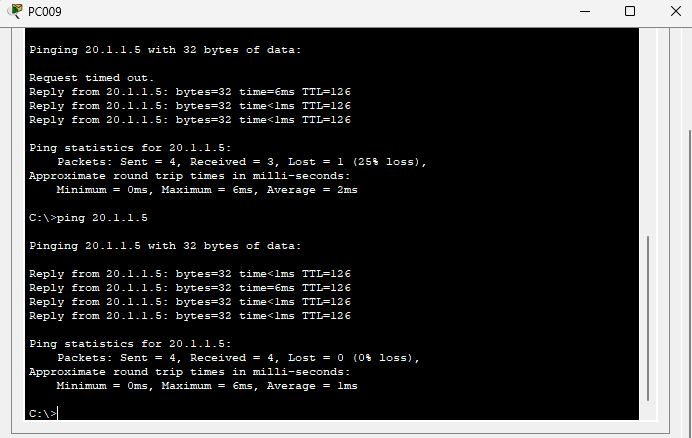
Testcase 006: When we ping from PC004(Vlan 20) to PC014(Vlan 40), we will get the replay successfully.



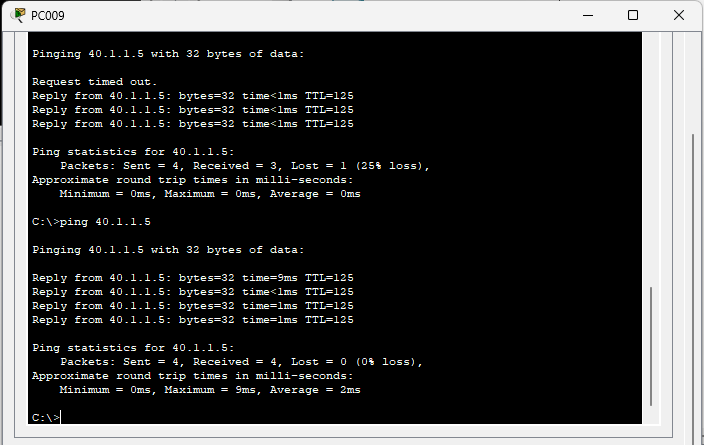
Testcase 007: When we ping from PC009(Vlan 30) to PC003(Vlan 50), we will get the replay successfully.



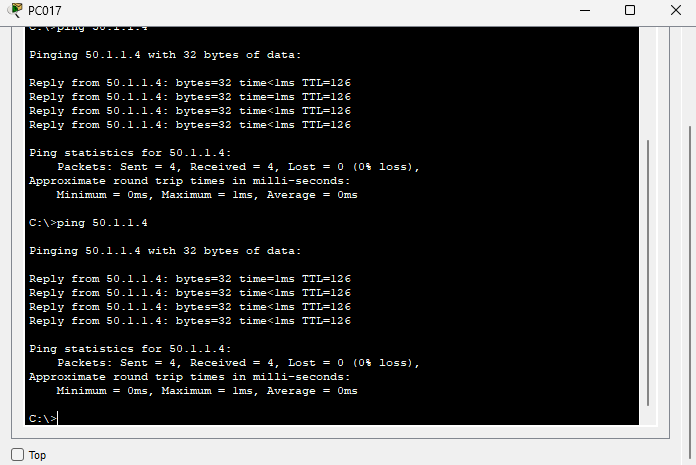
Testcase 008: When we ping from PC009(Vlan 30) to PC006(Vlan 20), we will get the replay successfully.



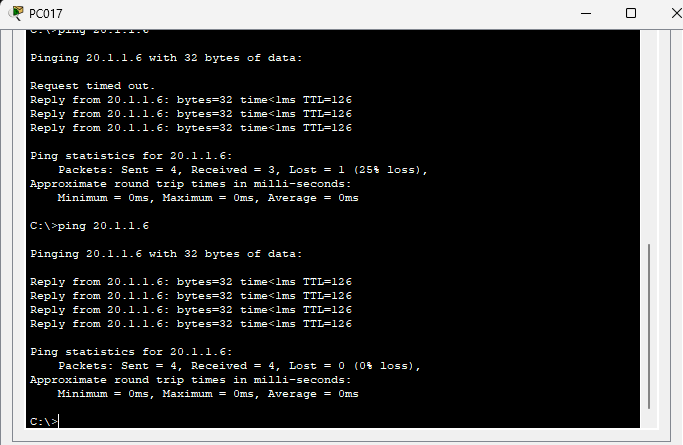
Testcase 009: When we ping from PC009(Vlan 30) to PC016(Vlan 40), we will get the replay successfully.



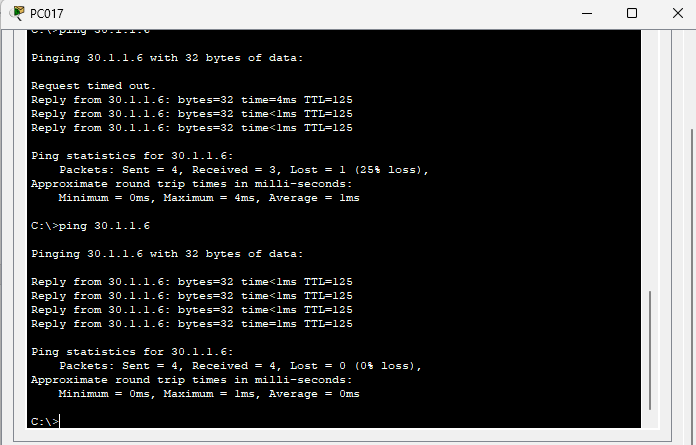
Testcase 010: When we ping from PC017(Vlan 40) to PC002(Vlan 50), we will get the replay successfully.



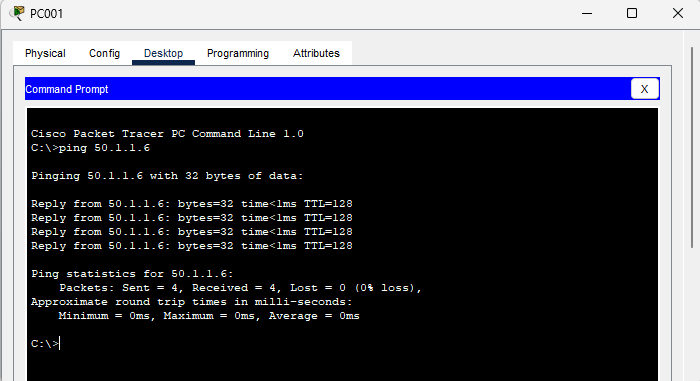
Testcase 011: When we ping from PC017(Vlan 40) to PC007(Vlan 20), we will get the replay successfully.



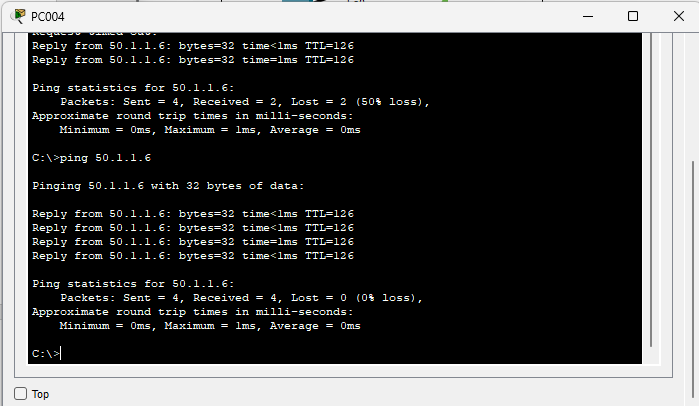
Testcase 012: When we ping from PC017(Vlan 40) to PC012(Vlan 30), we will get the replay successfully.



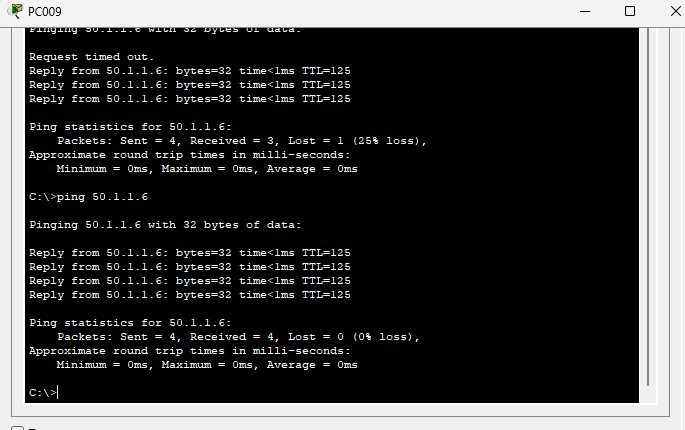
Testcase 013: When we ping from PC001 to Server1, we will get the replay successfully.



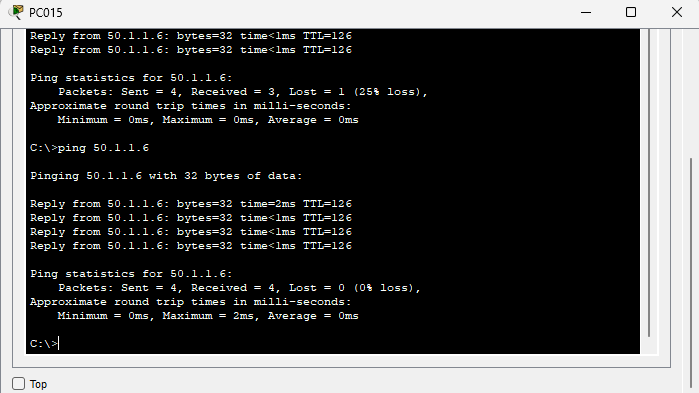
Testcase 014: When we ping from PC004 to Server1, we will get the replay successfully.



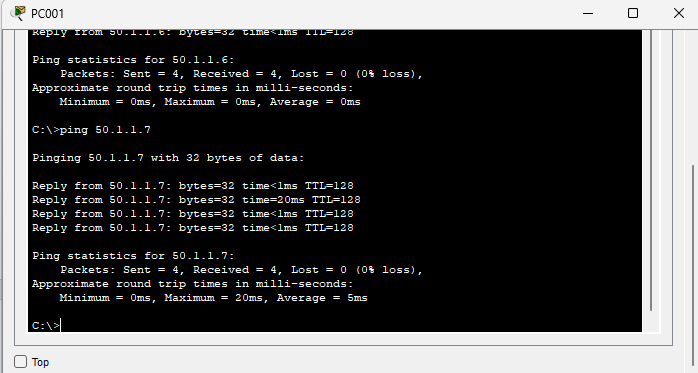
Testcase 015: When we ping from PC009 to Server1, we will get the replay successfully.



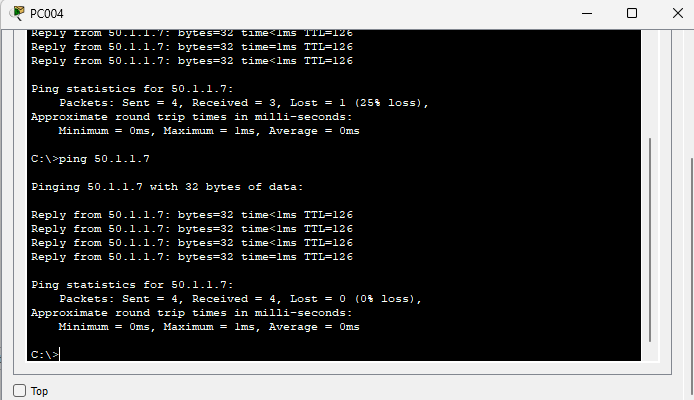
Testcase 016: When we ping from PC0015 to Server1, we will get the replay successfully.



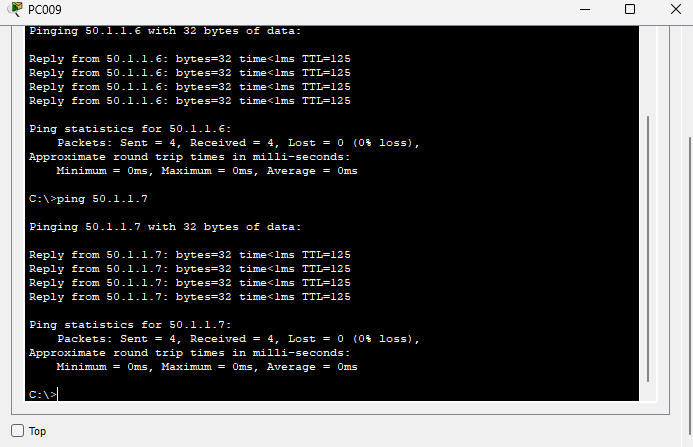
Testcase 017: When we ping from PC001 to Server2, we will get the replay successfully.



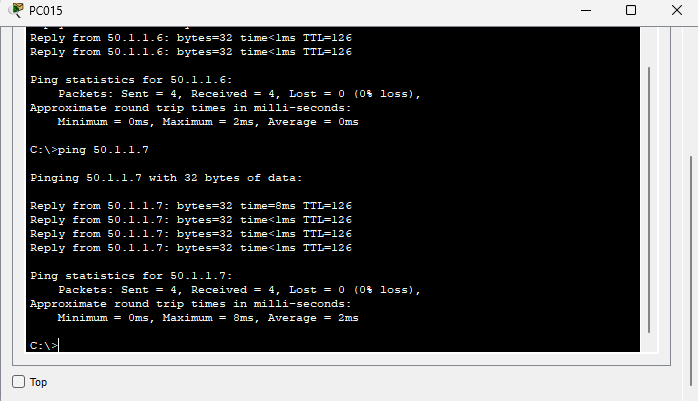
Testcase 018: When we ping from PC004 to Server2, we will get the replay successfully.



Testcase 019: When we ping from PC009 to Server2, we will get the replay successfully.



Testcase 020: When we ping from PC0015 to Server2, we will get the replay successfully.



# CHAPTER 4

## **4.1 CONCLUSION:**

As per the requirement given by the company named **Atlantic Connectify Solutions** the network topology is created with four VLAN’S each assigned to various department and the inter VLAN routing is enabled. The final output is verified by checking the connectivity of PC and servers from one VLAN to another VLAN using the Cisco Packet Tracer simulation tool and the output is verified by receiving successful ping response from the destination devices.

## **4.2 LINKS:**

Source Code: [GITHUB](https://github.com/Chodavaram-Sai-Bharath-Reddy/Group6Project)

PPT: [GoogleDocs](https://docs.google.com/presentation/d/1NXzV-VZMup2CLCEup0X_pmBAXt0B1OnhTXk6C20M2AM/edit?usp=sharing)