# COMPUTER NETWORK

# PROJECT REPORT

**ON**

# CISCO PACKET TRACER

**SUBMITTED TO : Dr. Mohammad Ahsan Chishti**

**SUBMITTED BY : ABHISHEK SHARMA**

Enrollment No. : 2020BCSE017

3rd year B.Tech (6th sem)



Department of Computer Science and Engineering National Institute of Technology Srinagar Srinagar, 190006

Title :

Cisco Switching Essentials:

1.Basic Configuration

2.VTP

3.VLANs

4.Security

5.EtherChannel

Abstract :

The project focused on essential aspects of Cisco switching, including basic configuration, VTP, VLANs, deny/allow VLANs, EtherChannel, and port security. The objectives were to understand and implement these features in a network environment. Methods involved configuring switches, setting up VLANs, utilizing VTP for VLAN propagation, managing VLAN access through deny/allow configurations, establishing EtherChannel for link aggregation, and implementing port security measures. The key findings include a comprehensive understanding of Cisco switching concepts, successful configuration of essential features, improved network performance, enhanced security through port access control, and efficient utilization of available network resources.

Introduction:

The project focuses on exploring and implementing various aspects of Cisco switching to enhance network performance and security. In modern network infrastructures, switches play a critical role in connecting devices and enabling efficient data transfer. However, configuring and managing switches effectively can be complex and challenging. This project aims to address these challenges by delving into key areas of Cisco switching and providing practical solutions.

Problem Statement:

Configuring Cisco switches and implementing advanced features can be daunting for network administrators. Understanding concepts such as VLANs, VTP, EtherChannel, and port security is crucial but often requires extensive knowledge and expertise. Furthermore, the lack of a comprehensive approach and practical examples can hinder efficient implementation and utilization of these features. Therefore, there is a need for a project that simplifies Cisco switching, provides clear guidance, and offers hands-on experience to overcome these challenges.

Objectives and Goals:

The primary objectives of this project are as follows:

Gain a thorough understanding of Cisco switching concepts and technologies.

Configure switches to optimize network performance and resource utilization.

Implement VLANs and VTP to simplify network management and facilitate efficient communication.

Establish secure access controls through deny/allow VLAN configurations and port security measures.

Set up EtherChannel to aggregate links and enhance network redundancy and bandwidth.

Motivation:

The motivation behind this project is to equip network administrators, IT professionals, and enthusiasts with the necessary knowledge and practical skills to configure and manage Cisco switches effectively. By providing clear explanations, practical examples, and step-by-step instructions, this project aims to simplify the implementation of essential Cisco switching features. The ultimate goal is to enhance network performance, improve security, and empower individuals to optimize their network infrastructures using Cisco switches.

Methodology/Approach:

The methodology used in this project involved a combination of theoretical study, practical implementation, and experimentation. The following tools, technologies, and techniques were employed:

Study and Research: Thorough study and research were conducted to understand the concepts and principles of Cisco switching, including basic configuration, VTP, VLANs, EtherChannel, and port security. Cisco documentation, textbooks, online resources, and official guides were utilized to gather in-depth knowledge.

Practical Implementation: Physical or virtual Cisco switches were used to set up a network environment for practical implementation. Various Cisco switch models, such as Catalyst switches, were deployed to simulate real-world scenarios. The configuration and management of switches were performed using the Command-Line Interface (CLI) or Graphical User Interface (GUI), depending on the available options.

Data Collection: Data collection involved gathering relevant information about network performance, security measures, and resource utilization before and after implementing specific features. This was done to evaluate the effectiveness of the implemented solutions and measure the impact on the network.

Experiments and Simulations: Experiments were conducted to test the behavior and performance of different features. For example, VLANs and VTP were implemented to observe the propagation of VLAN information across switches. EtherChannel configurations were tested to evaluate link aggregation and redundancy. Port security settings were applied to verify access control mechanisms.

Troubleshooting and Debugging: During the implementation phase, troubleshooting and debugging techniques were employed to identify and resolve any issues or errors that occurred. This involved analyzing log files, using debugging commands, and consulting documentation and online resources to find solutions.

Implementation:

**Part -1 : Basic Configurations**

* Draw the topology
* Make sure the connection between the switches take the first available interface while the connection between the switches and the PC’s can take rest.
* Configure the following –
* Hostnames
* Banner message(Unauthorised access prohibited)
* Privilege exec mode password(cisco)
* Line console password(cisco)
* Logging synchronous and execution time(2 mins)
* Line vty password(cisco)
* Logging synchronous and execution time(2 mins)
* Encrypt all the configured password
* Disable IP domain lookup
* Save configuration

**Part -2 : Etherchannel Configuration**

* Check the requirements including channel group,LACP protocols and ports to apply.
* Etherchannel should form and orange links should turn green.
* Test EtherChannel
* Do this for every switch .

**Part -3 : VTP Configurations**

* Configure the vtp domains to abcd.com
* Configure the vtp version to be 2
* Configure the vtp password to be cisco
* Switch 1 is to be vtp server and rest to be vtp client
* Verify if everything is configured correctly

**Part -4 : VLAN Configuration**

* Create 3 VLAN’s only in the VTP-SERVER-SWITCH as follows , VLAN 10-HR,

VLAN 20 -ICT, VLAN 30-FIN.

* In every switch(except for two in middle) designate Fa0/6-12 for VLAN 10,Fa0/13-19 for VLAN 20, Fa0/20-24 for VLAN 30.

Testing VTP

* Test VTP in every switch to see if all the vlan configuration are replicated or copied to all other VTP client switches use command do show vtp status.

Assigning IP addresses

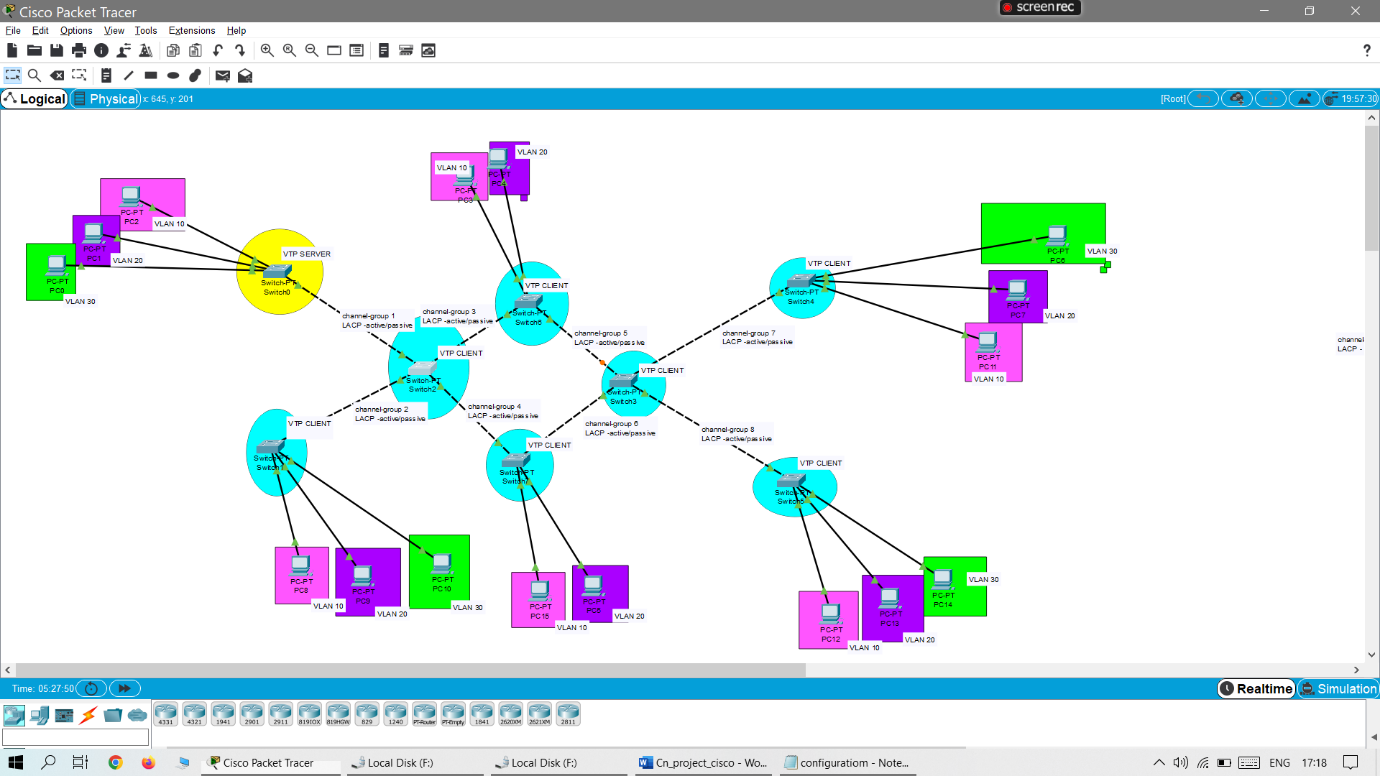
* Assign IP address to each PC and test the communication
* All devices should be assign IP address on this range 192.168.1.10-192.168.1.30 with a subnet mask of 255.255.255.0
* Make sure the computers are configured with correct IP address and those within the same VLAN can communicate.

**Part-5 : Switchport security configurations**

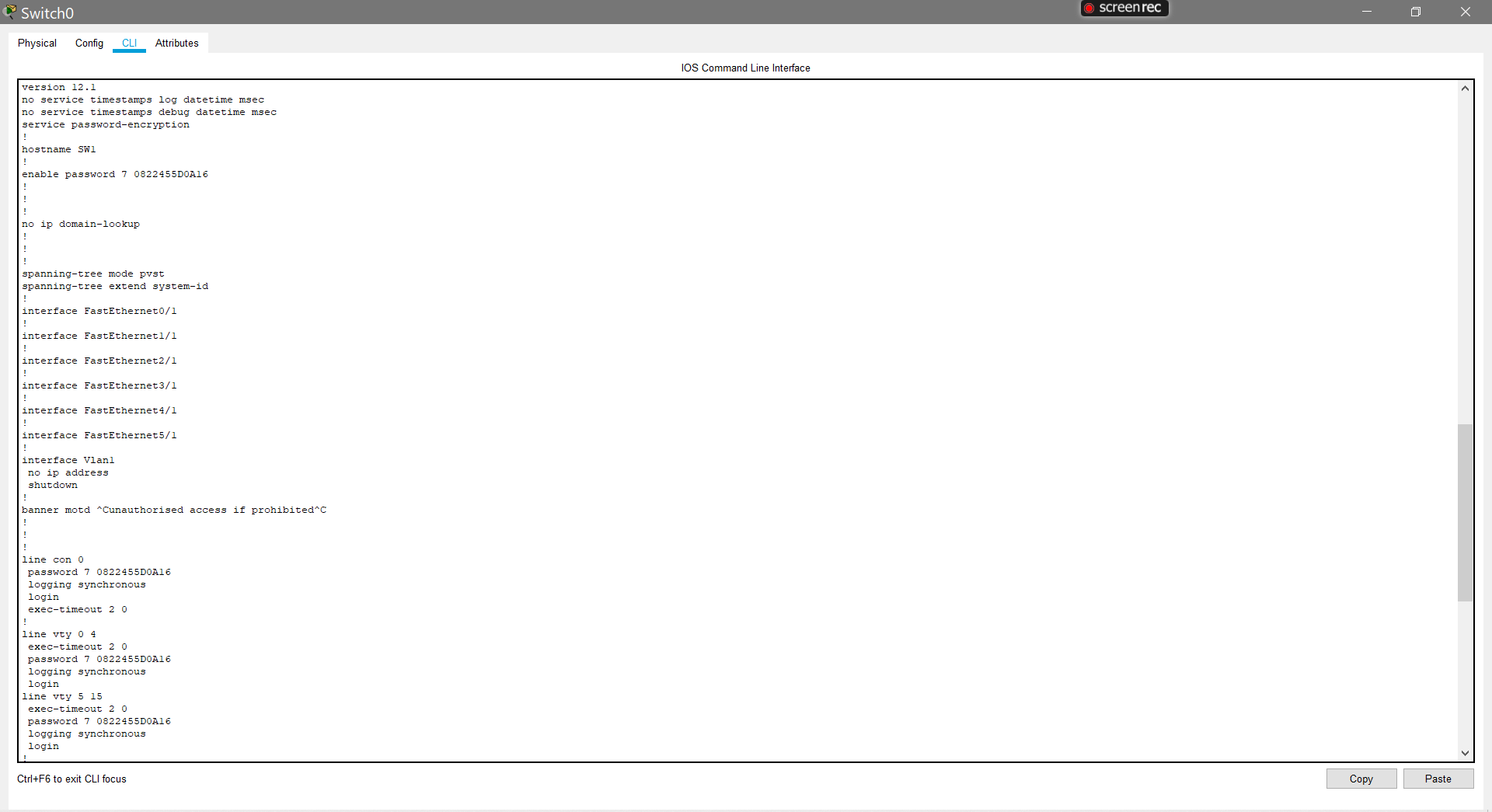
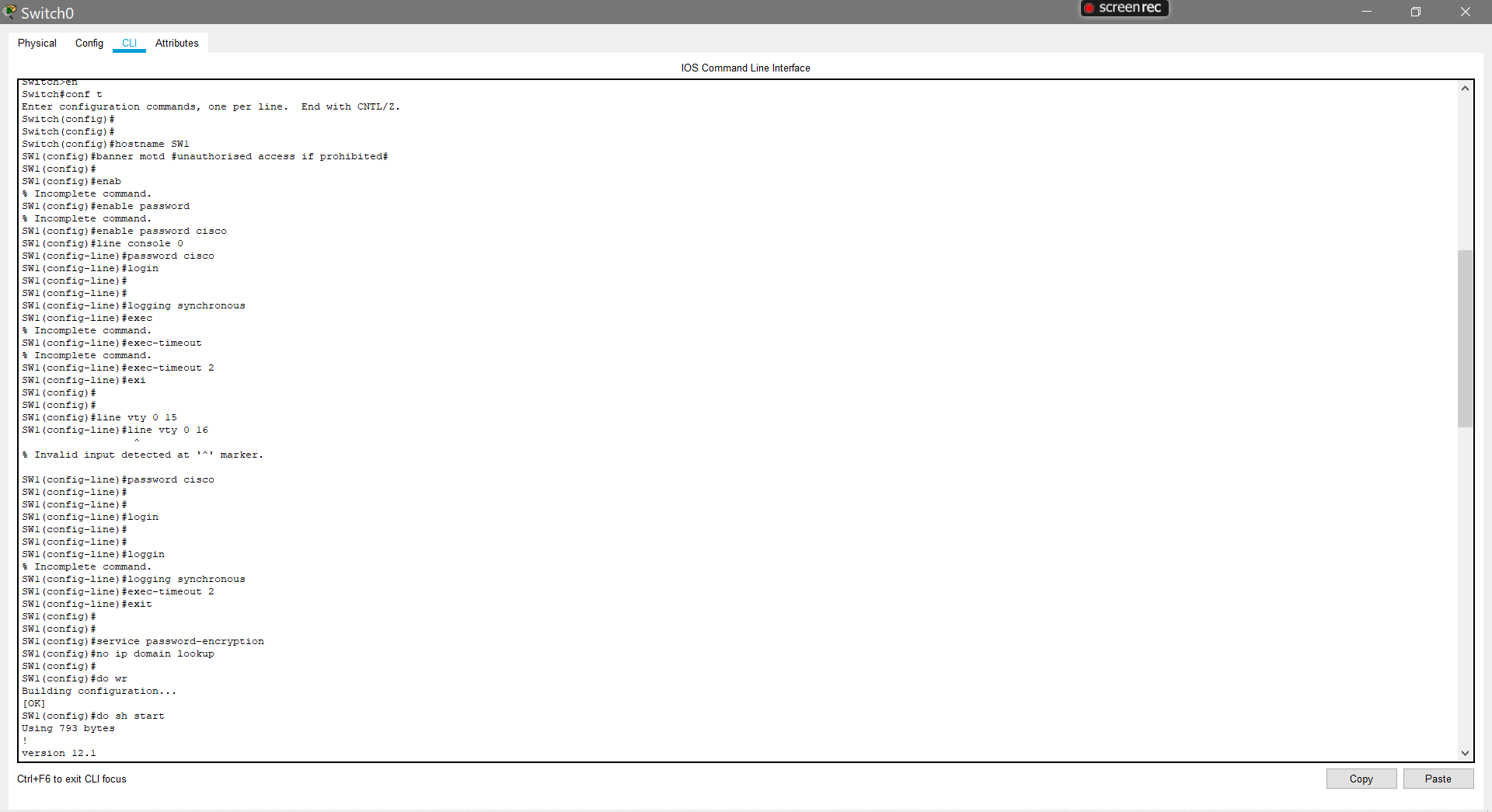
* In the switches, configure port security to allow a maximum of two MAC address per port.
* Configure sticky command to obtain MAC dynamically.
* Configure shutdown as the violation mode.

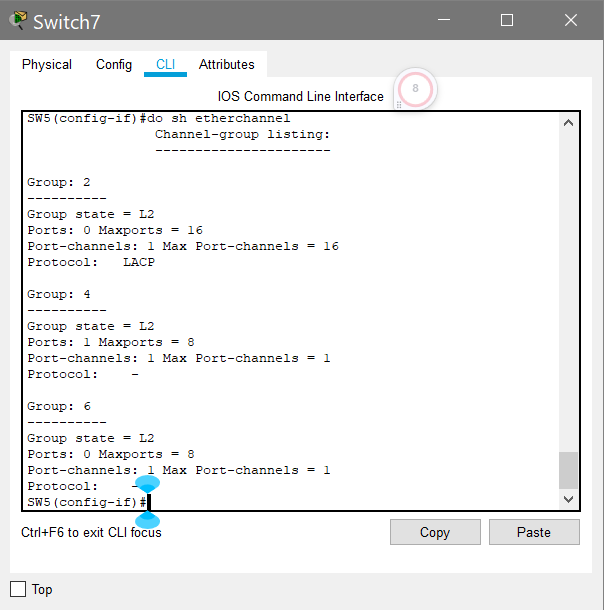
Result and analysis :

Establish cisco network-

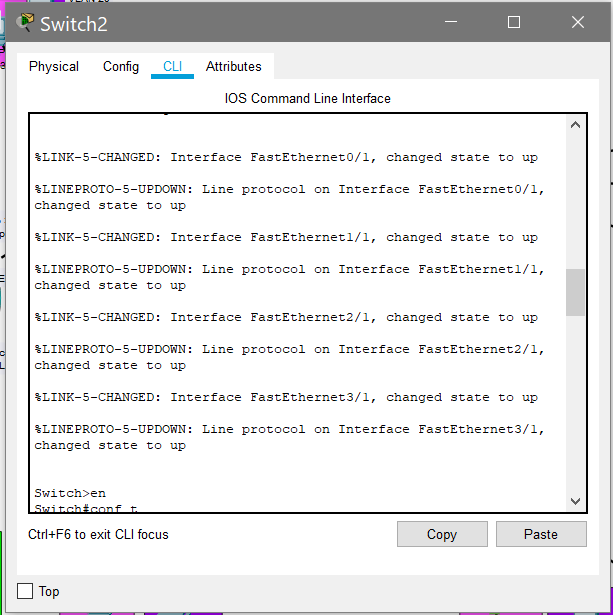


Basic configuration –

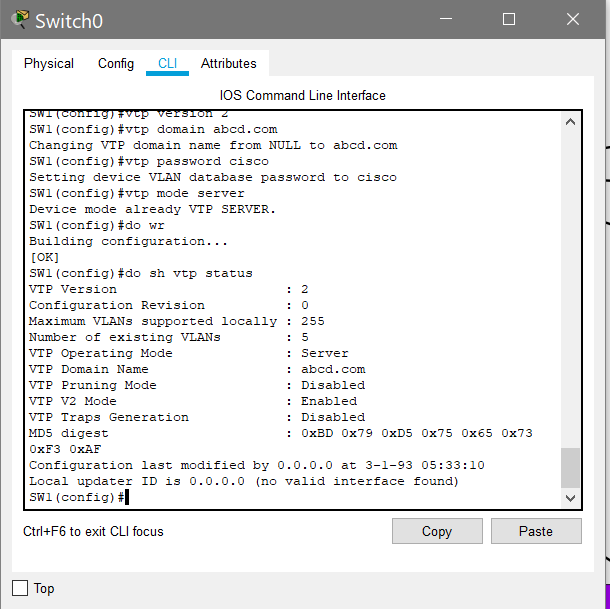


Etherchannel configuration –

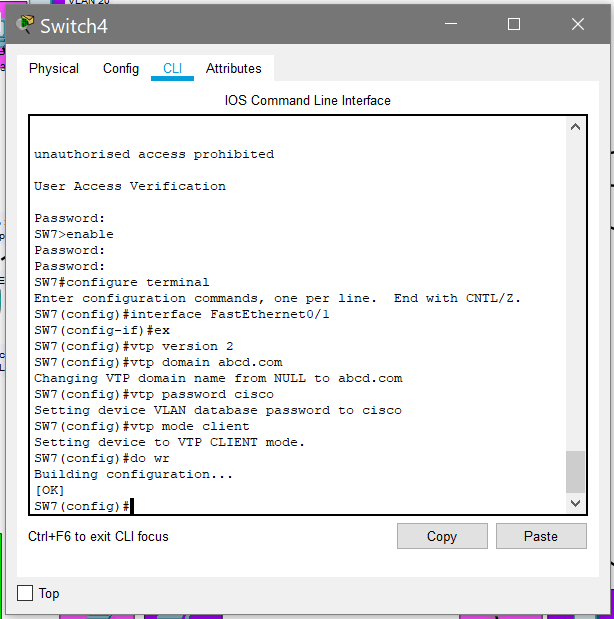
Changing LACP(Link Aggregation Control Protocol) states to active –



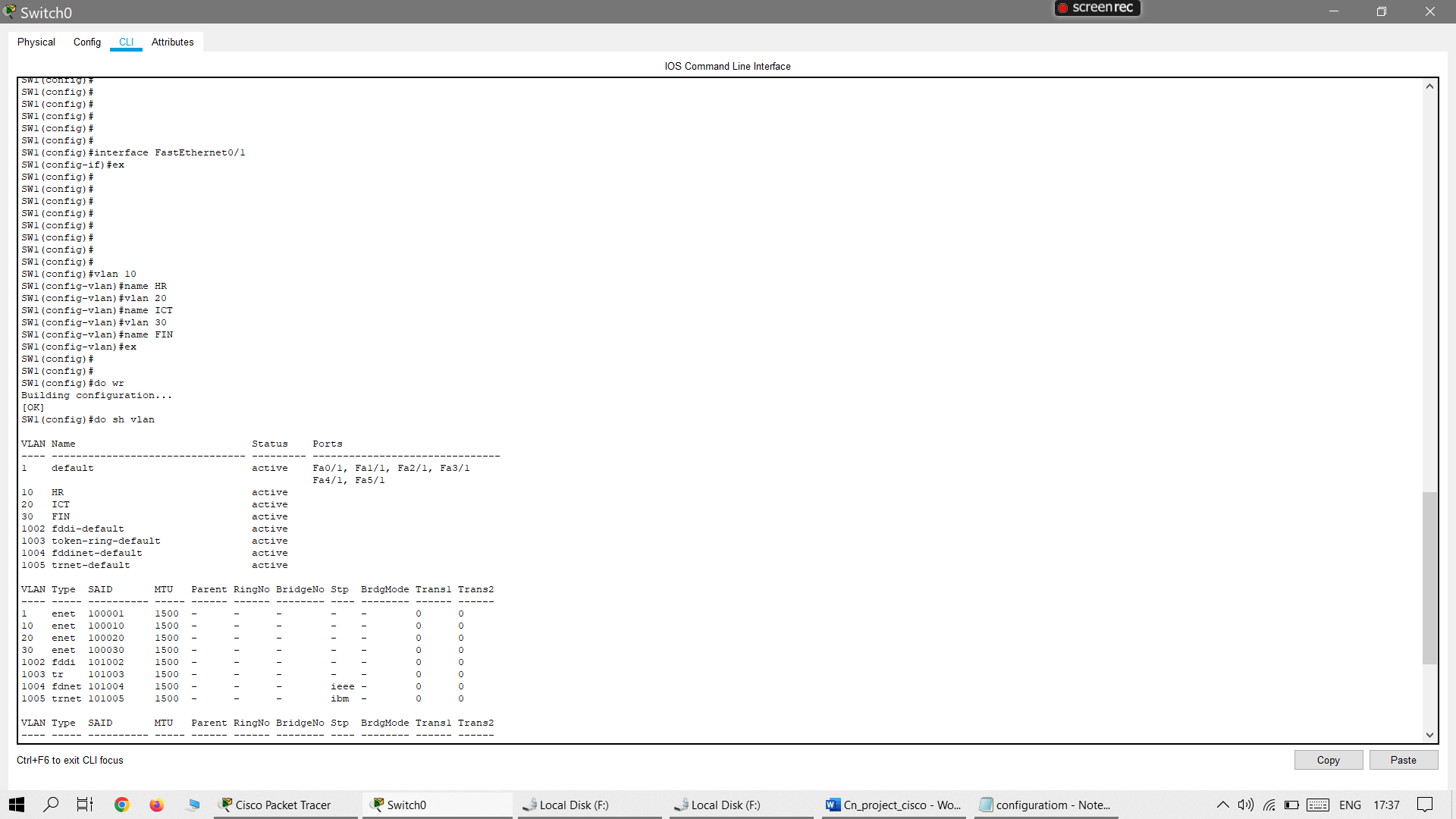
VTP Server Configuration –



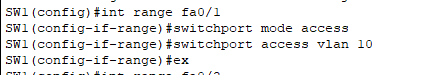
VTP client Configuration –



VLAN Configuration –

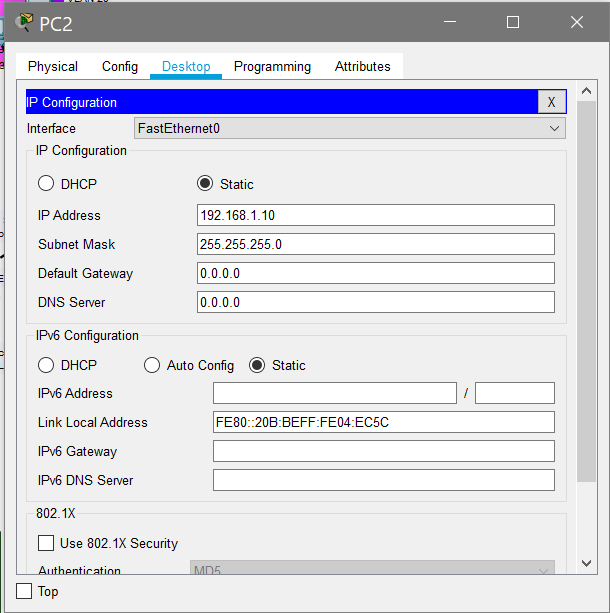


Server connecting to device(Allow VLAN) –

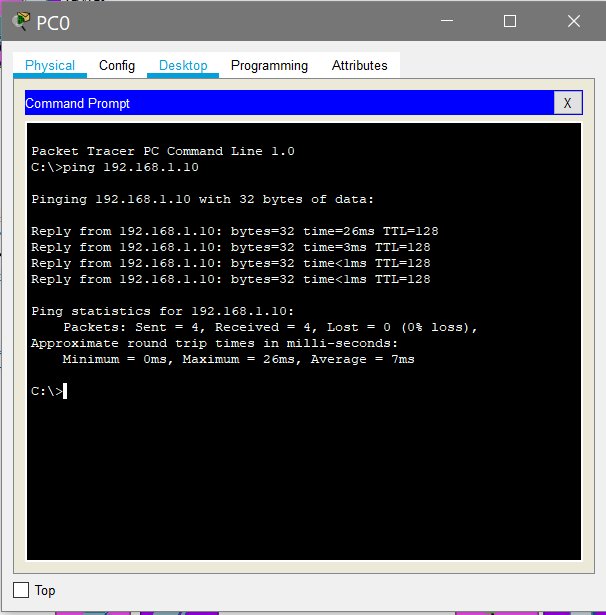




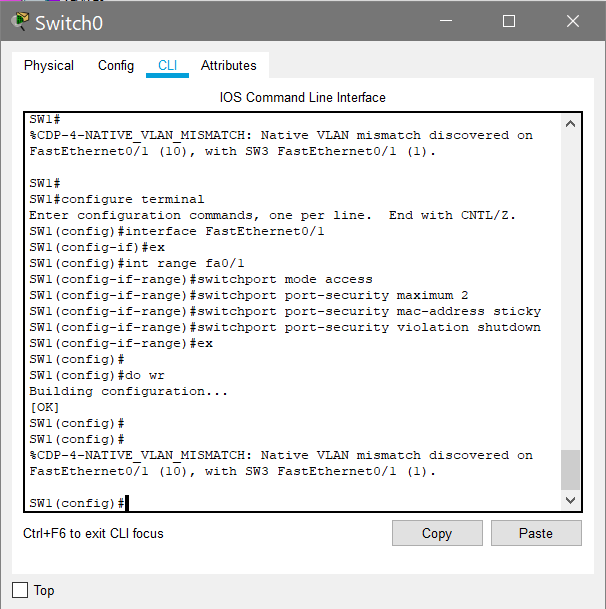
IP Configuration of devices –



Communication between devices –



SwitchPort Security -



Conclusion:

In conclusion, this project focused on Cisco Packet Tracer and covered various aspects of network configuration and security. The project began with basic configuration, which involved setting up devices, configuring IP addresses, and establishing connectivity. This foundation was crucial for building a functional network.

Next, the project delved into VLAN (Virtual Local Area Network) configuration. VLANs allow for logical segmentation of a network, improving performance, security, and manageability. Through Cisco Packet Tracer, the project demonstrated how to create VLANs, assign ports to VLANs, and implement inter-VLAN routing.

Furthermore, the project explored VTP (VLAN Trunking Protocol) configuration. VTP simplifies VLAN management by enabling automatic synchronization of VLAN information across multiple switches. The project showcased the process of configuring VTP domains, modes, and versions, ensuring consistent VLAN configurations throughout the network.

Another critical aspect addressed in this project was the implementation of access control in VLANs. By using the "deny" and "allow" VLAN commands, the project demonstrated how to restrict or permit traffic between VLANs. This capability is valuable for enhancing network security and isolating sensitive resources.

Finally, the project covered port security, which plays a vital role in preventing unauthorized access to switch ports. It explored various port security mechanisms, such as limiting the number of MAC addresses allowed on a port, configuring sticky MAC addresses, and enabling port security violation modes.

Overall, this project provided a comprehensive understanding of Cisco Packet Tracer and its capabilities for network configuration, VLAN and VTP management, and port security. By acquiring these skills, network administrators can effectively design, implement, and secure robust networks in a simulated environment, ensuring optimal performance and safeguarding critical resources.

References:

<https://www.youtube.com/@benardotom>

<http://www.cisco.com/warp/public/437/services/smartcallhome/>

http://cisco.com/en/US/products/hw/switches/ps708/products\_command\_reference\_book09186a0080160cd0.html