

Establishing a Secure Network System

By

Kaniz Fatima

152-15-5734

Md Toufiqur Rahman

152--15-5531

Anny Akter Shompa

152-15-5634

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering.

Supervised By

Dr.Fernaz Narin Nur

Assistant Professor

Department of CSE

Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

2 April 2019

APPROVAL

This Project titled “Establishing A Secure Network System”, submitted by Kaniz Fatima, ID No: 152-15-5734, Md Toufiqur Rahman, ID No: 152-15-5531, Anny Akter Shompa, ID No: 152-15-5634, to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on May 2, 2019.

BOARD OF EXAMINERS



Dr. Syed Akhter Hossain
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Chairman



Dr. Md. Ismail Jabiullah
Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Dr. Sheak Rashed Haider Noori
Associate Professor & Associate Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Dr. Md. Saddam Hossain Mukta
Assistant Professor
Department of Computer Science and Engineering
United International University

External Examiner

DECLARATION

We hereby declare that, this project has been done by us under the supervision of **Dr. Fernaz Narin Nur, Assistant Professor, and Department of CSE Daffodil International University**. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree.

Supervised by:

Fernaz

Dr. Fernaz Narin Nur

Assistant Professor

Department of CSE

Daffodil International University

Submitted by:

Kaniz Fatima

Kaniz Fatima

ID: 152-15-5734

Department of CSE

Daffodil International University

Md. Toufiqur R Rahman

Md. Toufiqur Rahman

ID: 152-15-5531

Department of CSE

Daffodil International University

Anny Akter Shompa

Anny Akter Shompa

ID: 152-15-5634

Department of CSE

Daffodil International University

©Daffodil International University

ACKNOWLEDGEMENT

First we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year project/internship successfully.

We would like to thank to supervisor of this project, **Dr.Fernaz Narin Nur, Assistant Professor**, Department of CSE Daffodil International University, Dhaka for the valuable guidance and advice. His willingness to motivate us contributed tremendously to our project. We also would like to thank him for showing us some example that related to the topic of our project. Besides, we would like to thank the authority of Daffodil International University for providing with a good environment and facilities to complete this project. I would like to express my gratitude towards my parents for their kind co-operation and encouragement which help me in completion of this project. We thanks and appreciations also go to our friend in developing the project and people who have willingly helped me out with their abilities.

We would like to express our heartiest gratitude to **Dr.Fernaz Narin Nur, Assistant Professor** and Head, Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

This project Title “Establishing a Secure Network System” is a communication system between intra office and branch office. Access Control List (ACL), Firewall and Virtual Private Network (VPN) are the most popular network security method. Hot Standby Routing Protocol (HSRP) is a modern process of network backup connection. For making the system more secure and realistic we use Port Address Translation (PAT). For controlling the redundancy of switches we have used Rapid Spanning-Tree Protocol (RSTP). After implementation of all the functions, the system is tested in several stages and it works successfully as a prototype.

TABLE OF CONTENTS	PAGE
CONTENTS	
APPROVAL	ii
BOARD OF EXAMINER	ii
DECLARATION	iii
ACKNOWLEDGEMENT	iv
ABSTRACT	v
CHAPTER 1: INTRODUCTION	1-2
1.1 Motivation	1
1.2 Objectives	2
1.3 Project Goal and Outcome	2
CHAPTER 2: BACKGROUND	3-7
2.1 Introduction	3
2.2 Literature Study	4
2.3 Comparative Studies	6
2.4 Scope of the Problem	6
2.5 Challenges	7
CHAPTER 3: REQUIREMENT SPECIFICATION	8-20
3.1 Introduction	8
3.2 VLAN	9
3.3 Inter VLAN	10

3.4 OSPF Routing protocol	11
3.5 PAT	12
3.6 ACL	13
3.7 DHCP	14
3.8 RSTP	16
3.9 HSRP	17
3.10 Firewall	18
3.11 SSH	19
3.12 Port security	20
CHPATER 4: DESIGN SPECIFICATION	21-33
4.1 Front-end Design	21
4.2 Back-end Design	22
4.3 Implementation Requirements	22
4.3.1 Simulator	22
4.3.2 GUI of Packet Tracer	23
4.3.3 Devices that we have used	24
CHAPTER 5: IMPLEMENTATION AND TESTING	25-41
5.1 Implementation	25
5.1.1 Assigning IP address into the pc	25
5.1.2 Assigning IP address into a router's port	26
5.1.3 Password protection system of router	27
5.1.4 Password protection system of switch	28

5.1.5 Configured VLAN	29
5.1.6 Configuration of VTP	30
5.1.7 Configuration of Inter-VLAN in L3 switch	31
5.1.8 Routing Protocols	32
5.1.8.1 Configuration of OSPF Routing protocol	32
5.1.8.2 Configuration of Static Routing protocol	33
5.1.8.3 Configuration of Default Routing	33
5.1.9 Configuration of Rapid Spanning Tree Protocol (RSTP)	33
5.1.10 Configuration of (HSRP) in Layer 3	34
5.1.11 Configuration of Access Control List (ACL)	35
5.1.12 Configuration of ASA Firewall	36
5.1.13 Configuration of PAT	39
5.1.14 Configuration of Port security	40
5.1.15 Configuration of VPN	41
5.2 Testing Implementation	42-60
5.2.1 Checking the running configuration	42
5.2.2 Checking the Routing:	47
5.2.3 Checking the VTP	48
5.2.4 Checking the RSTP	49
5.2.5 Checking the HSRP	50
5.2.6 Checking the port security	51

CHAPTER 6: CONCLUSION AND FUTURE SCOPE	52
6.1 Discussion and Conclusion	52
6.2 Scope for Further Developments	52
REFERENCES	53

List of Figures

FIGURES	PAGE
Figure 3.1: VLAN	9
Figure 3.2: Inter VLAN	10
Figure 3.3: OSPF	11
Figure 3.4: Port Address Translation	12
Figure 3.5: Access Control List	13
Figure 3.6: Dynamic Host configuration protocol	14
Figure 3.6: Process of obtaining IP address from DHCP server	15
Figure 3.7: Spanning Tree Protocol (STP)	16
Figure 3.8: Hot Standby Routing Protocol	17
Figure 3.9: Firewall	18
Figure: 4.1: Front-end design	21
Figure 4.2: GUI of packet Tracer	23
Figure 5.1: Assigning IP address in pc	25
Figure 5.2: Assigning IP address in routers port	26
Figure 5.3: Password protection system of Router	27
Figure 5.4: Password protection system of Switch	28
Figure 5.5: Configuration of Basic VLAN	29
Figure 5.6: Configuration of VTP	30
Figure 5.7: Configuration of Inter VLAN in layer 3 switch	31
Figure 5.8: Configuration of OSPF Routing protocol	32
Figure 5.9: Configuration of HSRP	34

Figure 5.10: Configuration of ACL	35
Figure 5.11: Configuration of ASA Firewall Part 1	36
Figure 5.12: Configuration of ASA Firewall Part 2	37
Figure 5.13: Configuration of ASA Firewall part 3	38
Figure 5.14: Configuration of PAT	39
Figure 5.15: Configuration of Port Security	40
Figure 5.16: Configuration of VPN	41
Figure 5.17: checking the running configuration part 1	42
Figure 5.18: checking the running configuration part 2	43
Figure 5.19: checking the running configuration part 3	44
Figure 5.20: checking the running configuration part 4	45
Figure 5.21: checking the running configuration part 5	46
Figure 5.22: checking the routing	47
Figure 5.23: checking the VTP	48
Figure 5.24: checking the RSTP	49
Figure 5.25: checking the HSRP	50
Figure 5.26: checking the Port Security	51

List of Tables

TABLE	PAGE
Table 2.1: Literature Study	4-6

CHAPTER 1

INTRODUCTION

Secure network system is required to communicate between employees of head office and branch offices. Without a secure communication system it is impossible to share private information.

Now a days, security violation of network has become a common term. Unauthorized access is the reason for this problem. For this reason secure communication system is a demand of modern era. In corporate world wants security of their information.

For this aim we need to establish a secure network system.

1.1 Motivation of Secured Communication

Now-a-days many communications system take place over a long distance and treated by technology and increasing consciousness about the importance of security issues and technology. Unauthorized access is really harmful for our communication. For this reason, secured communication focuses on every sector of our modern technology. In corporate world every organization wants security of their information or data which they want to share with their authorized departments. For this purpose we developed a system for “**Secure Network**”.

1.2 Project Objective

The project is designed to make a secure communication system among to branches of a company. Organizations are connected via Virtual private Network (VPN). Network rules are created. Traffic maintaining their rules can access the specific service. By using VPN, VLAN, ACL, Firewall we can ensure a secured network system. By this secure connection organization can share their private information without any intrusion.

1.3 Project Goal and Outcome

Data security is a very import issue for everyone. Everyone wants to keep their data free from unauthorized access. Our “Establishing a Secured network System” provides better security and also provides connections redundancy between employee of the same office and employees of the branches office. We are trying to ensure the data security.

In this project we developed a Communication System which provides security between one LAN To other LAN

CHAPTER 2

BACKGROUND STUDY

2.1 Introduction:

Computer Network refers to the connection of some devices in such a way so that they can communicate with each other. There are many types of computer network like LAN (Local Area Network), WAN (Wide area Network) and so on. LAN refers to a small area network and WAN refers to the network that covers huge area.

A secure network refers to a network that is free from intrusion, surveillance and eavesdropping. A fully secure network does not exist in the real world. Network can be 99% secure but if anyone says “it is 100% secure network” this term is nothing but a false statement.

2.2 Literature Study

We read many research papers. The main part of some research papers are given in the table 2.1

TABLE: 2.1 LITERATURE STUDY

I. no.	Research Paper	Author Name	Methodology	Description	Outcome
1.	Modern Network Security: Issues and Challenges	Shailja Pandey Department of Information Technology, BBDNITM Uttar Pradesh Technical University, Lucknow, India	1. Cryptography 2. Firewall i) Application gateway ii) Packet filtering iii) Hybrid system	In this paper Author has been described the necessary measures and specification regarding large organizational requirements for establishing a secure network. Wifi networks are very familiar to provide wireless networks. So its need of different provisions to handle the threats of wifi and hacking pursuit.	The author have been shown the minimum set of specification framework to create a secure network of any organization. He used very little of methods for that reason this system is not flexible.

2.	Securing the Network Perimeter of a Community Bank	Steven M. Launius	<ol style="list-style-type: none"> 1. Routing 2. NAT 3. Firewall 4. Stateful Inspection Firewall(SIF) 5. Proxy Firewall 6. Static Packet Filtering 7. VPN 8. PBX 9. VoIP 10. RAS 	<p>In this paper author wants to raise appreciation of the external threats present to intimate customer information retained on the private network of community bank. They wants to design a protected perimeter of network.</p>	<p>The secure Network perimeter is very important for us. The solutions granted are Industry are best method that IT Security specialist used to contribute any network with perimeter security.</p>
3.	Building a Secure Local Area Network	Tamirat Atsemegeorgi	<ol style="list-style-type: none"> 1. Basic configuration of network devices 2. Securing the inside network using firewall 3. Securing switch 4. Securing Remote Client Access 5. Securing the wireless connection 	<p>Author tried for designing a LAN for a small organization and studying sensitivity of the system and measuring Gadget security to assure network and organization benefits.</p>	<p>For building a secured network system, a network administrator demands to select the right type of technology which is fitting with the company's target and security requirements. Here he was using very less of methodology.</p>

2.3 Comparing Study

We were reading many research papers. Every research paper has some problems that's why another research paper will come. Many of the research papers, we found that the author were using very little methods for security but we are using here a lot of methodology for ensuring organization's security. We are using here Access Control List (ACL), Virtual Private Network (VPN), Virtual Local Area Network (VLAN), Inter VLAN, Open Shortest Path First (OSPF), Port Address Translation (PAT), Rapid Spanning Tree Protocol (RSTP), Firewall etc. We are trying ensure a more secures network in any organizations.

2.4 Two scope of problem:

Now a days almost every day we hear news about hacking and leaking. Many more network system are getting hacked because of their some small vulnerabilities. If we can ensure our own LAN security, hacking possibilities of our LAN will greatly reduce. In real life everyone is really concern about only their virtual security. That's why they use many additional software. Sometimes this software can create backdoor and let the hackers in. We have tried to ensure both virtual, topological and physical security without using any additional software hence we used the default security system of network devices. It is a matter of sorrow that someone consider their system as 100% secure. But actually no system is 100% secure. So we are trying to harden the security to make the system difficult to hack.

2.5 Challenges:

It is a very challenging project. Collecting network pattern of a corporate office is not an easy task. No office wanted to share their network topology. Besides the simulation software is supporting a very less functionalities of Firewall. And sometimes firewall act weird on packet tracer. It not change its routing configuration no matter how many time the configuration is removed and re write the configuration again. It takes a lot of effort and time to reach this sustainable state of our network system because of the simulator. But we hope that challenges would be favorable to us in professional life

CHAPTER 3

REQUIREMENT SPECIFICATION

3.1 Introduction

This chapter describe about the requirement function of network topology. Which function we add and for what purpose we are using this.

We have added:

1. VLAN
2. Inter-VLAN
3. ACL
4. PAT
5. OSPF
6. ACL
7. DHCP
- 8 .RSTP
9. HSRP
10. Firewall
11. VoIP
12. VPN
13. SSH
14. Port security

3.2 VLAN

VLAN refers to Virtual Local Area Network. It refers to a group of device that are connected with each other on one or more LANs. VLANs are based on logical in reverse of physical connection. It uses layer 2 network. VLANs operate the data link layer of OSI model. [1] We have shown VLAN in figure 3.1

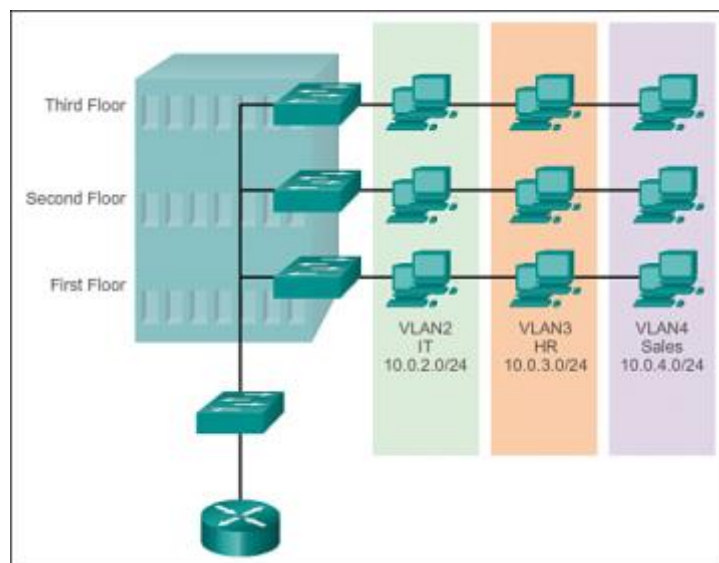


Figure 3.1: VLAN

Why we have used VLAN in our network system?

We have used VLAN for separate the department of our topology and increasing security. By using VLAN we can control traffic patterns and react swiftly to employee or equipment relocation. Without VLAN users appoint networks based on geology and are limited by objective topologies and distances. VLANs serve network segmentation.

3.3 Inter-VLAN

Inter-VLAN is a routing process which ensures the communication between different VLAN. In figure 3.2 we have shown the inter VLAN

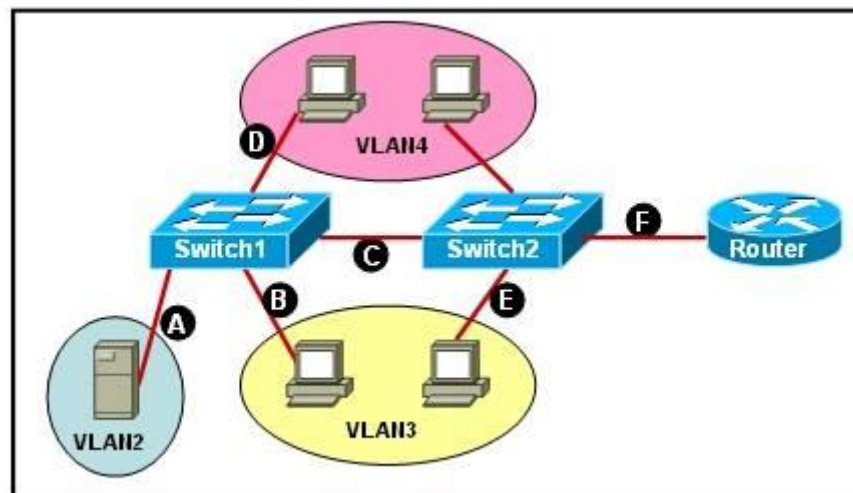


Figure 3.2: Inter VLAN

Why we have use Inter VLAN in our network system?

Works with almost all switches cause the switches do not have to backing layer 3, only VLANs

And trunking. For communicate between every VLAN we have used Inter VLAN.

3.4 OSPF Routing Protocol

The full form of OSPF is Open Shortest Path First. This Routing protocol finds the best path for forwarding packets among the connected networks. OSPF has RIP support for building in both for router to host communication and for unity with older networks using RIP as their fundamental protocol. We have shown the OSPF Routing in figure 3.3

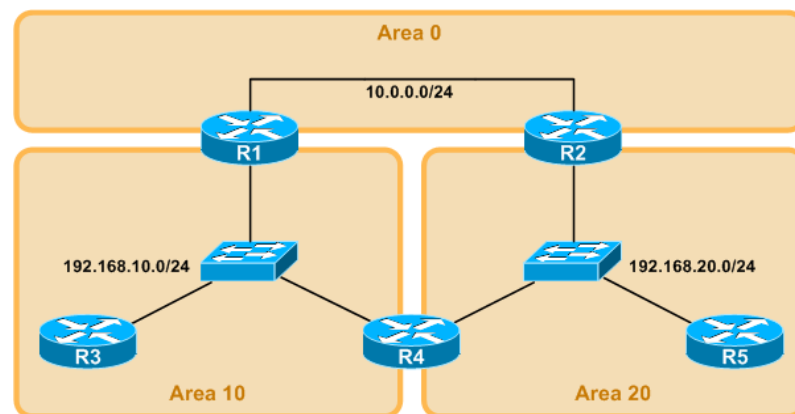


Figure 3.3: OSPF

Why we have used OSPF in our network system?

OSPF is a link state routing protocol. When configured OSPF, It will listen to neighbors and collect all link state data available to create a topology map of all accessible paths in its network and then save the instruction in its topology database, also known as Link State Database (LSD).

3.5 What is PAT?

The full form of PAT is Port Address Translation. It is a part of Network Address Translation (NAT). It allowed multiple private IP generalized with a single Public IP. We have shown PAT in figure 3.4

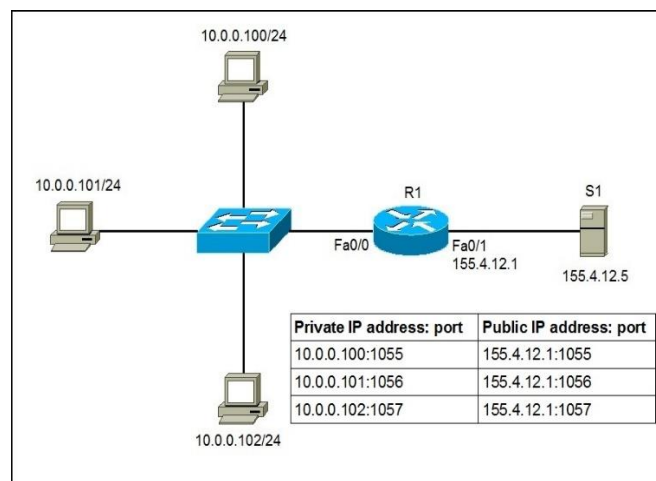


Figure 3.4: Port Address Translation

Why we have use Inter PAT in our network system?

- Increasing security.
- Private to public and public to private address translation.

3.6 What is ACL?

The full form of ACL is Access Control List. It is used for controlling the access of traffic

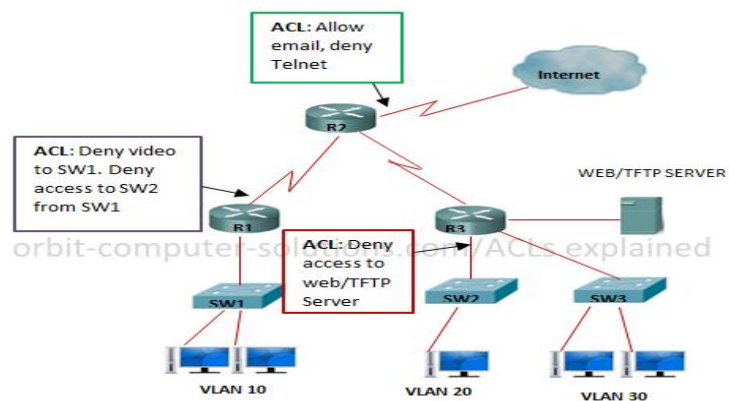


Fig 3.5: Access Control List

Why We Use ACL?

There are many reasons for using ACL. Like

The main reason is ACL provides us security in networking. It provides more protection on higher speed interfaces where line rate speed is necessary and firewall may be anta logistic. It is also used for restricting updates to route from network peers. [2]

3.7 What is DHCP?

DHCP refers Dynamic Host configuration protocol .It is a process by which all hosts are assigned IP address automatically. For this we need a DHCP server that will provide the IP addresses and DHCP clients. DHCP clients will request for an IP address to the DHCP server. If IP address available then DHCP server will provide an IP address to that client. We have shown the connection between DHCP server and client in figure 3.6

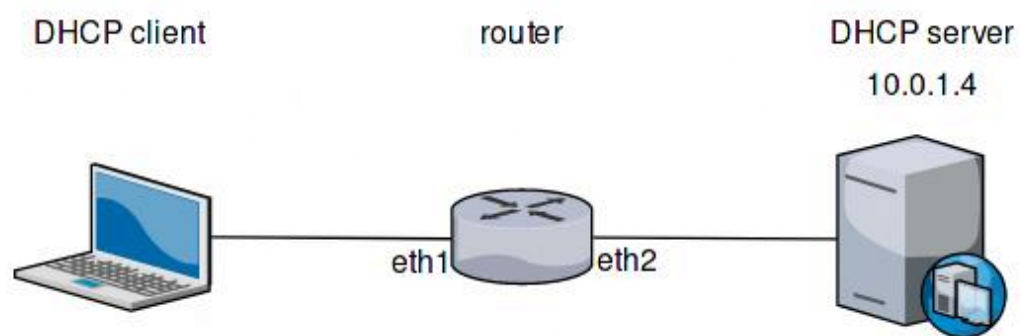


Figure 3.6: Dynamic Host Configuration Protocol (DHCP)

How DHCP server works?

DHCP connection establish by handshaking between DHCP client and DHCP server.

The phases of this process are

1. Discovery
2. Offer
3. Request
4. Acknowledgement

The handshaking process is given in figure 3.7

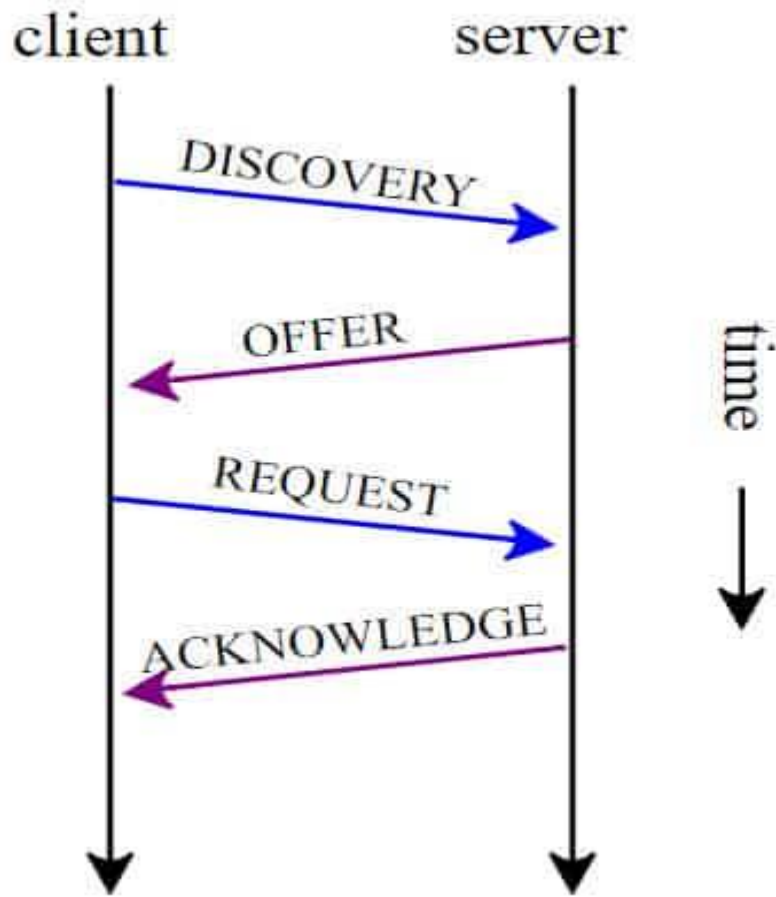


Figure 3.7: Process of obtaining IP address from DHCP server

1. Discover: Client Search for DHCP server. This discovery method is Broadcast
2. Offer: DHCP server send offer to client. By this DHCP server shows its presence.
3. Request: After getting the offer the client request for an IP address from DHCP server
4. Acknowledgement: DHCP server assigned IP address to that client and send acknowledgement.

3.8 Rapid Spanning-Tree Protocol (RSTP):

RSTP is the better version of STP that is used to control the loop between switches. When some switches are connected to each other, loop is also created between them. By that loop switches send broadcast message all the time. If this process continue for a long time then the switch will run out its memory and the network will be very slow or can be the network can go down.

RSTP virtually disconnect the link that is creating loop though physically they are connected. By this it saves the network from congestion. It follows 802.1w IEEE standard where STP follow 802.1d. We have shown the RSTP in figure 3.8

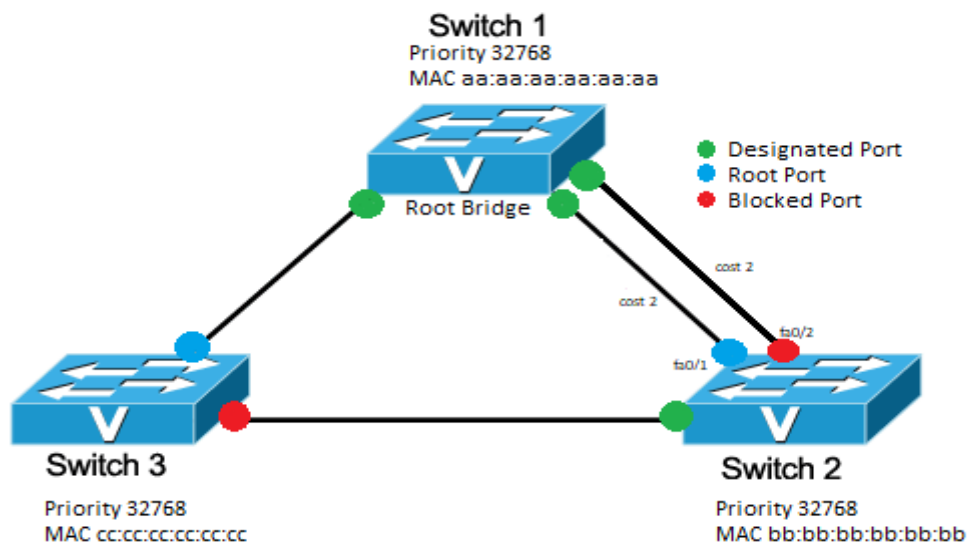


Figure 3.8: Spanning Tree Protocol (STP)

Why we use RSTP in our topology?

1. Broadcast Storm:
2. Mac address instability
3. Multiple copies of Frame

3.9 Hot Standby Router Protocol (HSRP):

Hot standby router protocol is a process by which we can manage two routers by keeping one in active mode and another one in standby mode. The active router transmit the packets from the LAN to internet. But if router 1 unable to send the packets for it's any kind of failure then the standby router2 become active and send the packets to internet. If the router 1 snap out its problem and become active then the router 2 again goes to standby mode and router 1 become active.

We have shown HSRP in figure 3.9

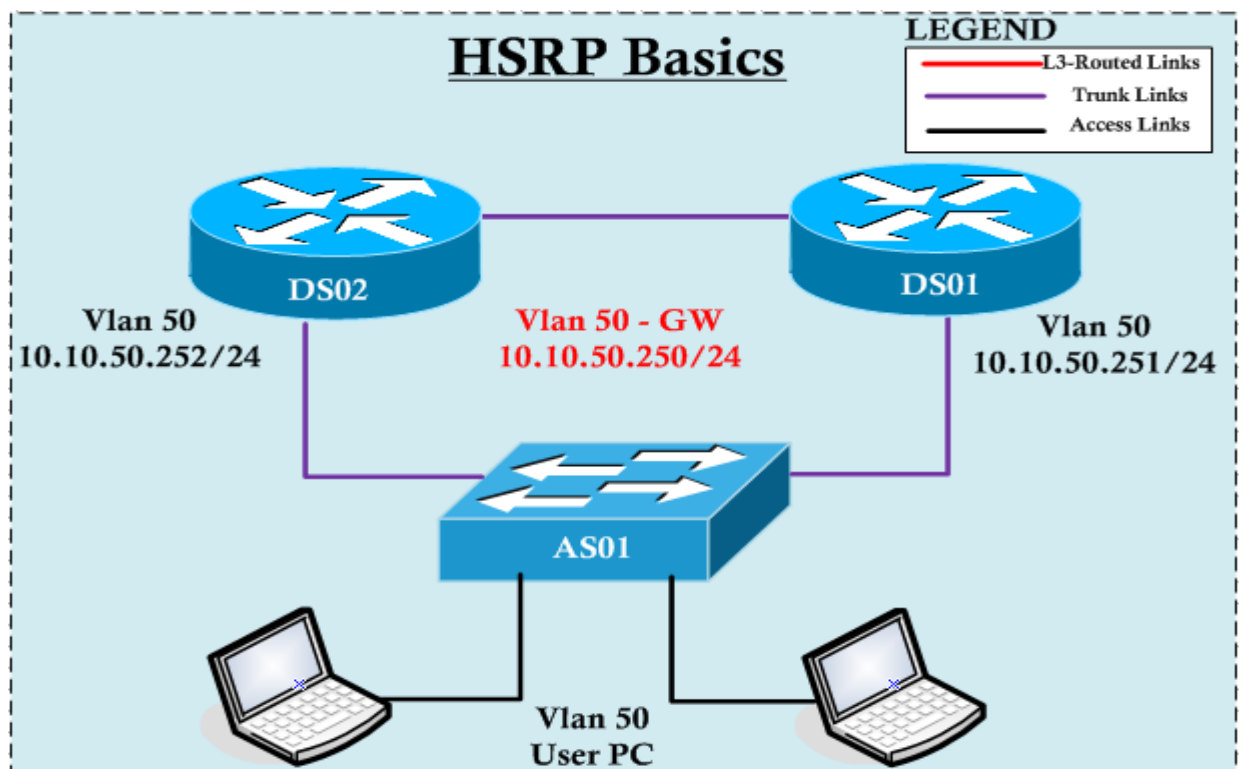


Figure 3.9: Hot Standby Routing Protocol

Why we have used HSRP in our topology?

1. Network stability is maintained by it
2. Data passing guaranty can be given

3.10 Firewall:

Firewall refers to a network security device that inspect incoming and outgoing traffic. By its inspection if it thought that any traffic from the LAN or to the LAN trying violating its security rules that had been set by a network admin, it block that traffic. Firewall can be hardware or software. Some firewall have both. [3] In figure 3.10 we have shown the Firewall of network

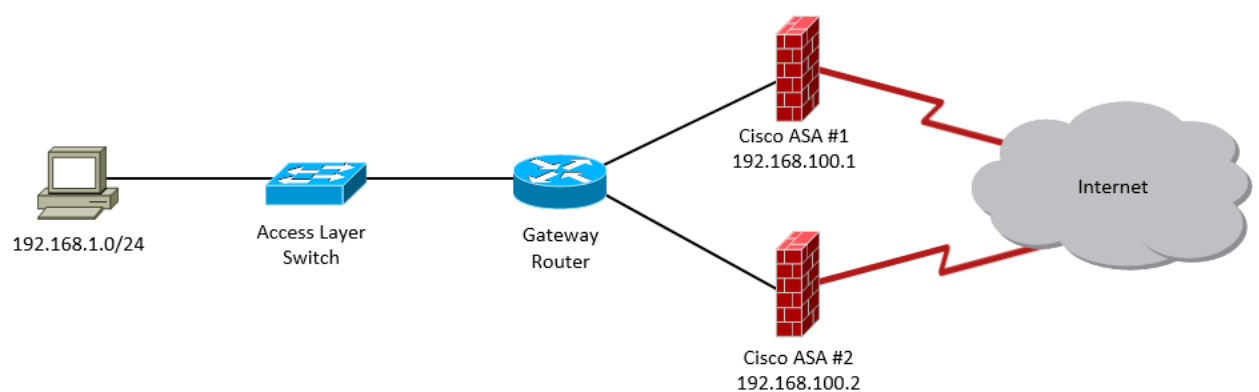


Figure 3.10: firewall

Why we have used firewall? :

The reason of use firewall is given below

1. enhancing security
2. protecting the resources of LAN
3. inspection and validating incoming or outgoing traffic
4. Giving record of its all activity

3.11 SSH

Secure shell SSH protocol is used to secure the remote login. SSH was designed to replace the unsecure remote connection Telnet. Secure shell Provides Strong authentication and encryption of communication between two computers

Why we have used SSH in our topology?

- Provides stronger authentication system. Check traffic by secret private keys
- Password is less secure than SSH
- Non-interactive login

3.12 Port security:

Port security is a process by which we can prevent intruder end devices to connect with our network .In this process switches learn the mac address of the connected computers. If any new-fangled end device is added through any of the existing Ethernet cable, and try to send any packet in the network , switch will immediately shutdown that new end device connected port. So the new device won't be able to connect with the network.

Why we have used Port security?

1. Increasing security
2. Maintaining Bandwidth

CHAPTER 4

DESIGN SPECIFICATION

This chapter will describe about the designing process of our project.

4.1 Front-end Designing:

As it is a packet tracer based networking project that's why for designing the front-end we have use some network devices with some network topologies. Then we have to connect them according to our topology. We have used different type of wire to connect the devices with one another.

We have shown our projects front-end Design in figure 4.1

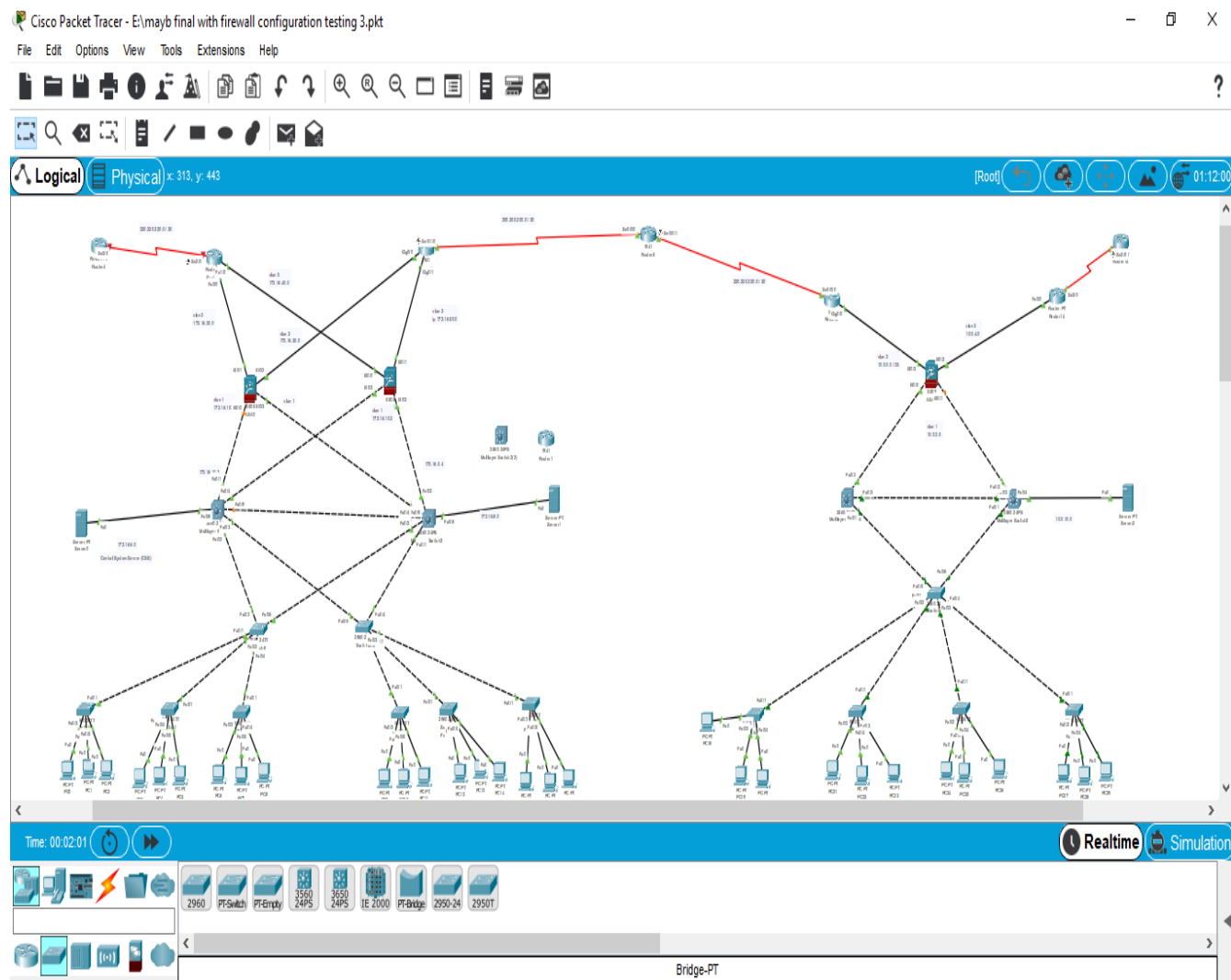


Figure 4.1: front-end design

4.2 Back-end design:

For networking project back-end is designed by some configuration code so that the topology works perfectly.

4.3 Implementation Requirement:

As it is a simulating software that's why we need the simulator software to implement our system. And then we need the pre-installed network devices and their accessories to implement our project

4.3.1 Simulator

Cisco Packet Tracer

Cisco packet tracer is a wonderful software that enables us to visualize our network and implement those creative network design. This software is developed by CISCO system. [7]

4.3.2 GUI of packet tracer: We have shown the graphical user interface of packet tracer in figure 4.2

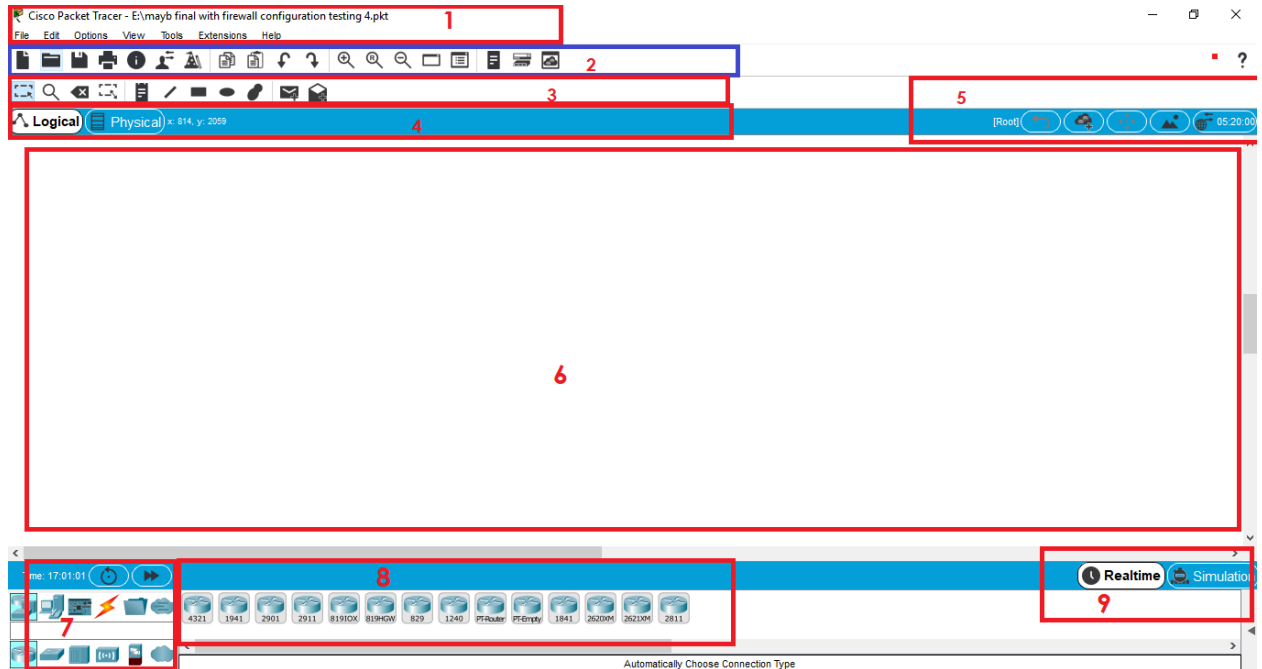


Figure 4.2: GUI of packet tracer

1. Menu Bar
2. Main tool Bar
3. Common tool bar
4. Logical or Physical environment bar
5. Accessories tab
6. Workspace
7. Network devices
8. Device types selection box
9. Real-time or simulation mode bar

4.3.3 The devices that we have used to design our network

1. Router: Router is an OSI model's layer 3 device. We have use the different models of cisco router. Like generic and 1941 series router.
2. Switch: there are mainly two types of switch. OSI Layer 2 and OSI layer 3 switch. Among the different versions of layer 2 switches we have use 2960T switch 3560

And among different versions of layer 3 switches we have use 3650-24ps switch

3. Firewall: Firewall is layer 3 device. It is used to inspect traffic from inside to outside or outside to inside
4. End device: we have used pc as our end device.
5. Wire: We have used different types of wire for different purpose.

The wire that we have used

1. Fast Ethernet cable
2. Gigabit Ethernet cable
3. Serial cable
6. Server: Server is a special device that supports many protocols. Like HTTP, FTP,SMTP,DCHP,TFTP

CHAPTER 5

Implementation

5.1.1 Assigning IP address into the pc:

We have shown IP assigning in pc in figure 5.1

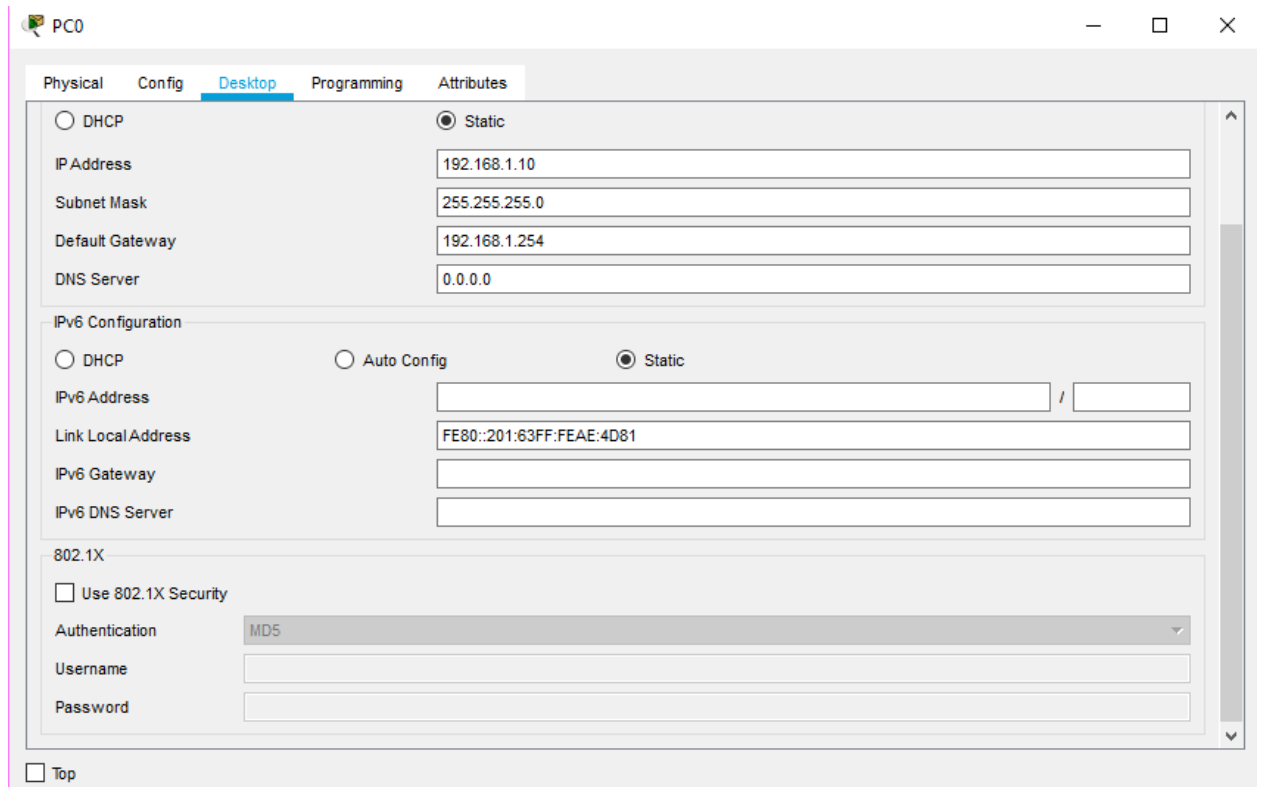
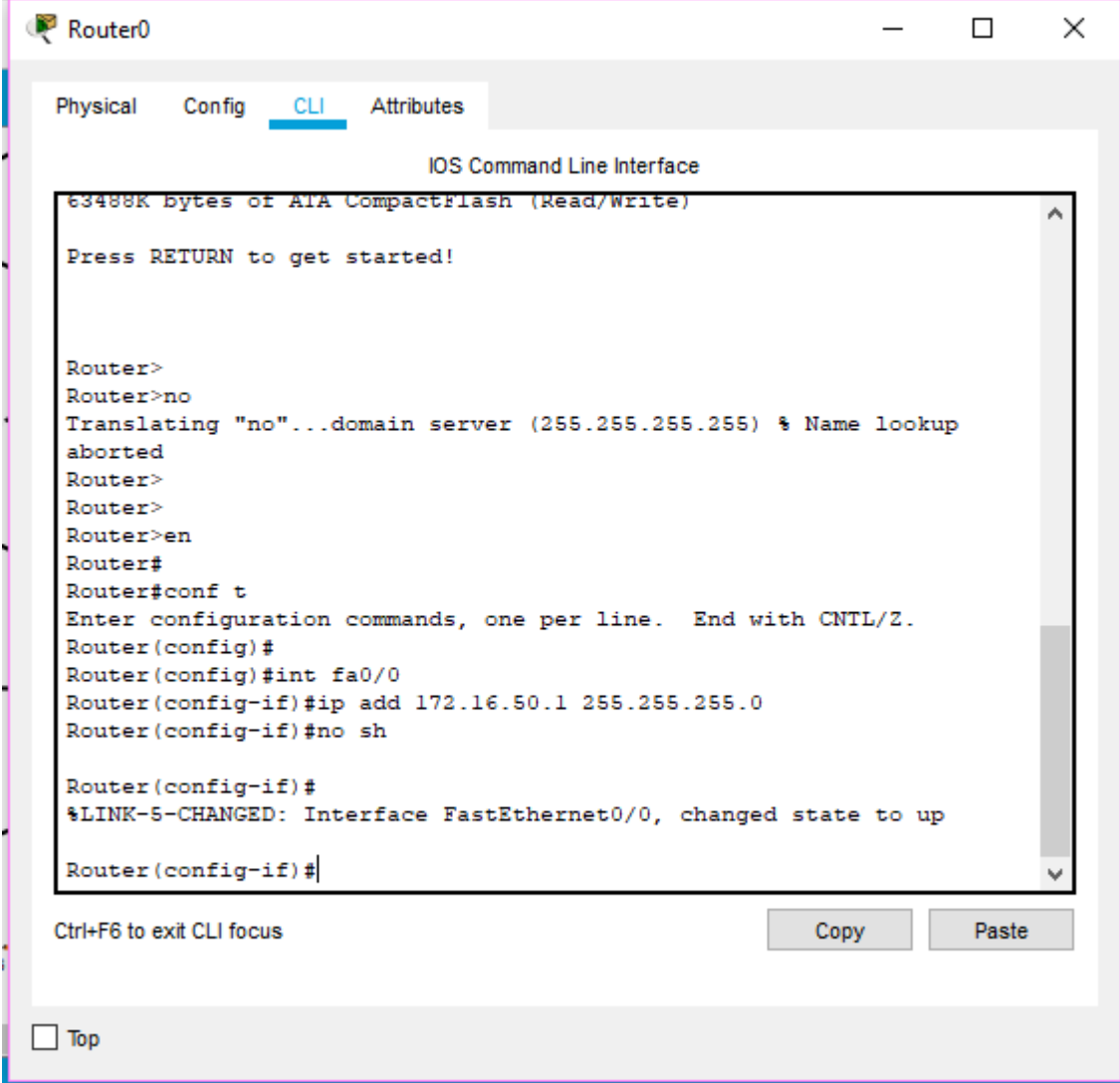


Figure 5.1: IP assigning in pc

5.1.2 Assigning IP address into a router's port:

We have shown IP assigning in router in figure 5.2



```
Router0
Physical Config CLI Attributes
IOS Command Line Interface
63488K bytes of ATA CompactFlash (Read/Write)
Press RETURN to get started!

Router>
Router>no
Translating "no"...domain server (255.255.255.255) % Name lookup
aborted
Router>
Router>
Router>en
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#int fa0/0
Router(config-if)#ip add 172.16.50.1 255.255.255.0
Router(config-if)#no sh

Router(config-if)#
%LINK-S-CHANGED: Interface FastEthernet0/0, changed state to up

Router(config-if)#
```

Ctrl+F6 to exit CLI focus

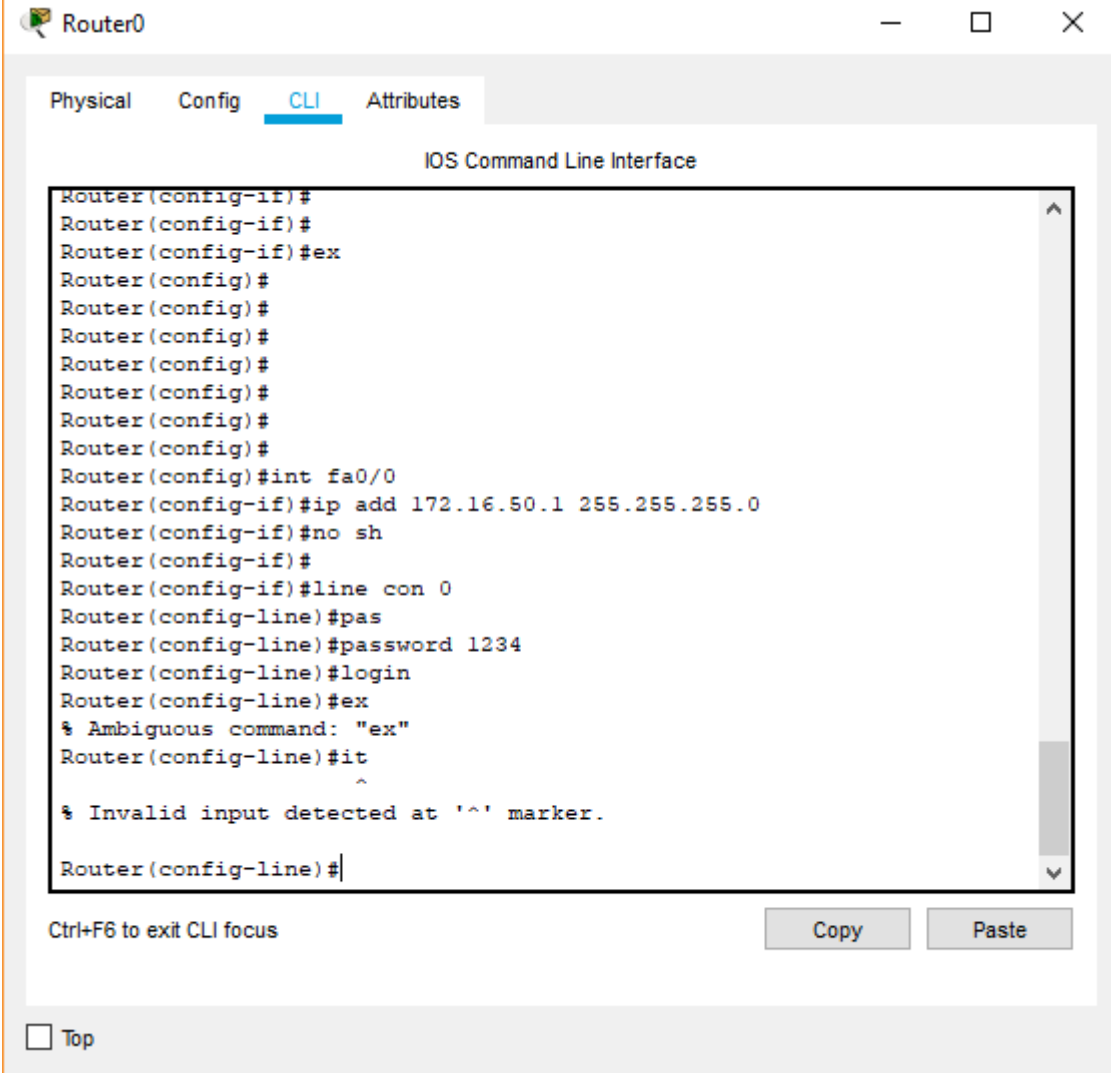
Copy Paste

Top

Figure 5.2: IP assigning in pc

5.1.3 Password protection system of router:

We have shown configuration of password protection system of router in figure 5.3



```
Router0
Physical Config CLI Attributes
IOS Command Line Interface
Router(config-if)#
Router(config-if)#
Router(config-if)#ex
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#int fa0/0
Router(config-if)#ip add 172.16.50.1 255.255.255.0
Router(config-if)#no sh
Router(config-if)#
Router(config-if)#line con 0
Router(config-line)#pas
Router(config-line)#password 1234
Router(config-line)#login
Router(config-line)#ex
% Ambiguous command: "ex"
Router(config-line)#it
^
% Invalid input detected at '^' marker.
Router(config-line)#
```

Ctrl+F6 to exit CLI focus

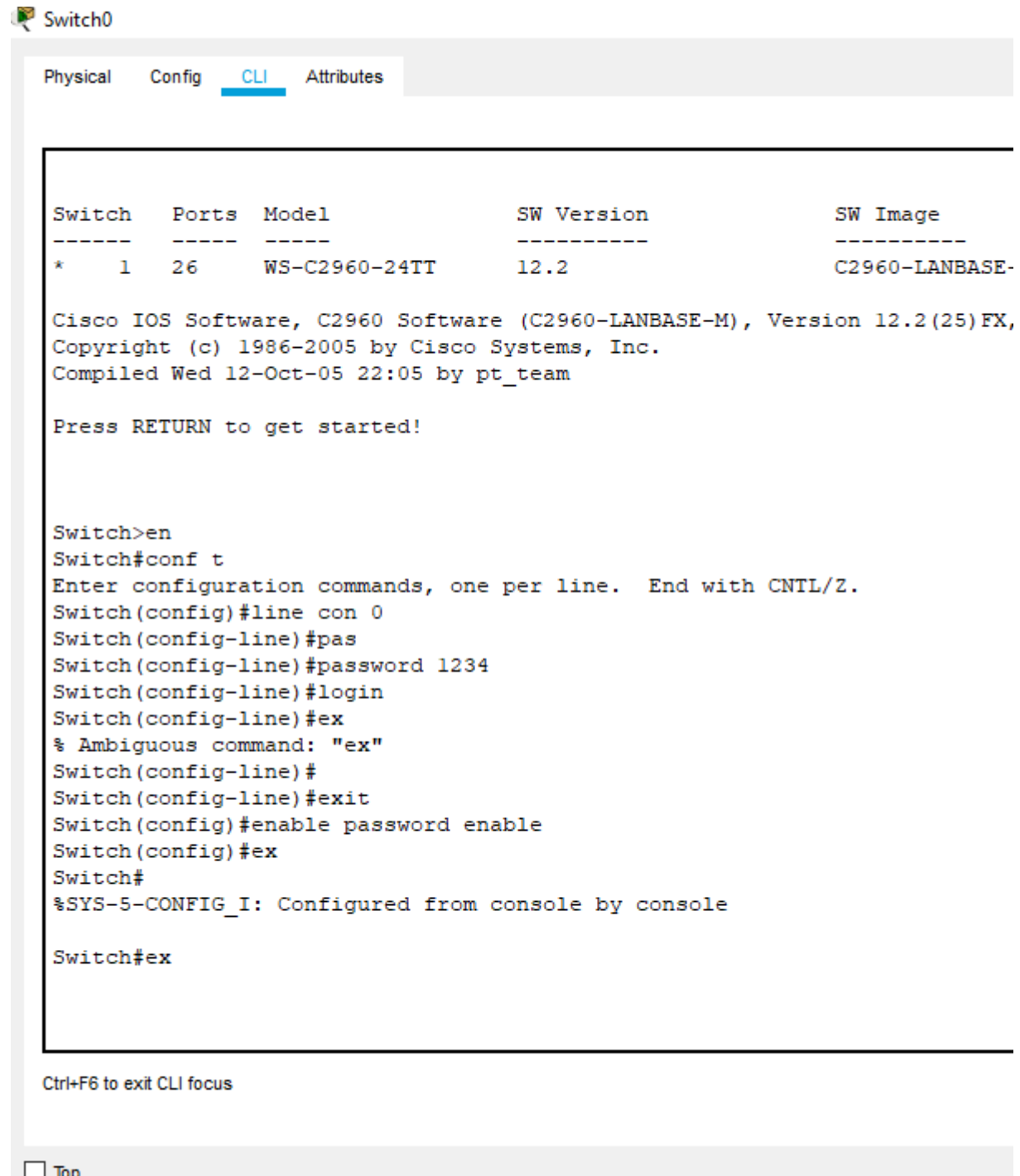
Copy Paste

Top

Figure 5.3: Password protection system of Router

5.1.4 Password protection system of switch:

We have shown the configuration of password protection system of switch in figure 5.4



The screenshot shows a Cisco switch CLI interface with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the following output:

```
Switch  Ports  Model          SW Version      SW Image
-----  -
*    1    26    WS-C2960-24TT    12.2            C2960-LANBASE-

Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX,
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

Press RETURN to get started!

Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#line con 0
Switch(config-line)#pas
Switch(config-line)#password 1234
Switch(config-line)#login
Switch(config-line)#ex
% Ambiguous command: "ex"
Switch(config-line)#
Switch(config-line)#exit
Switch(config)#enable password enable
Switch(config)#ex
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#ex
```

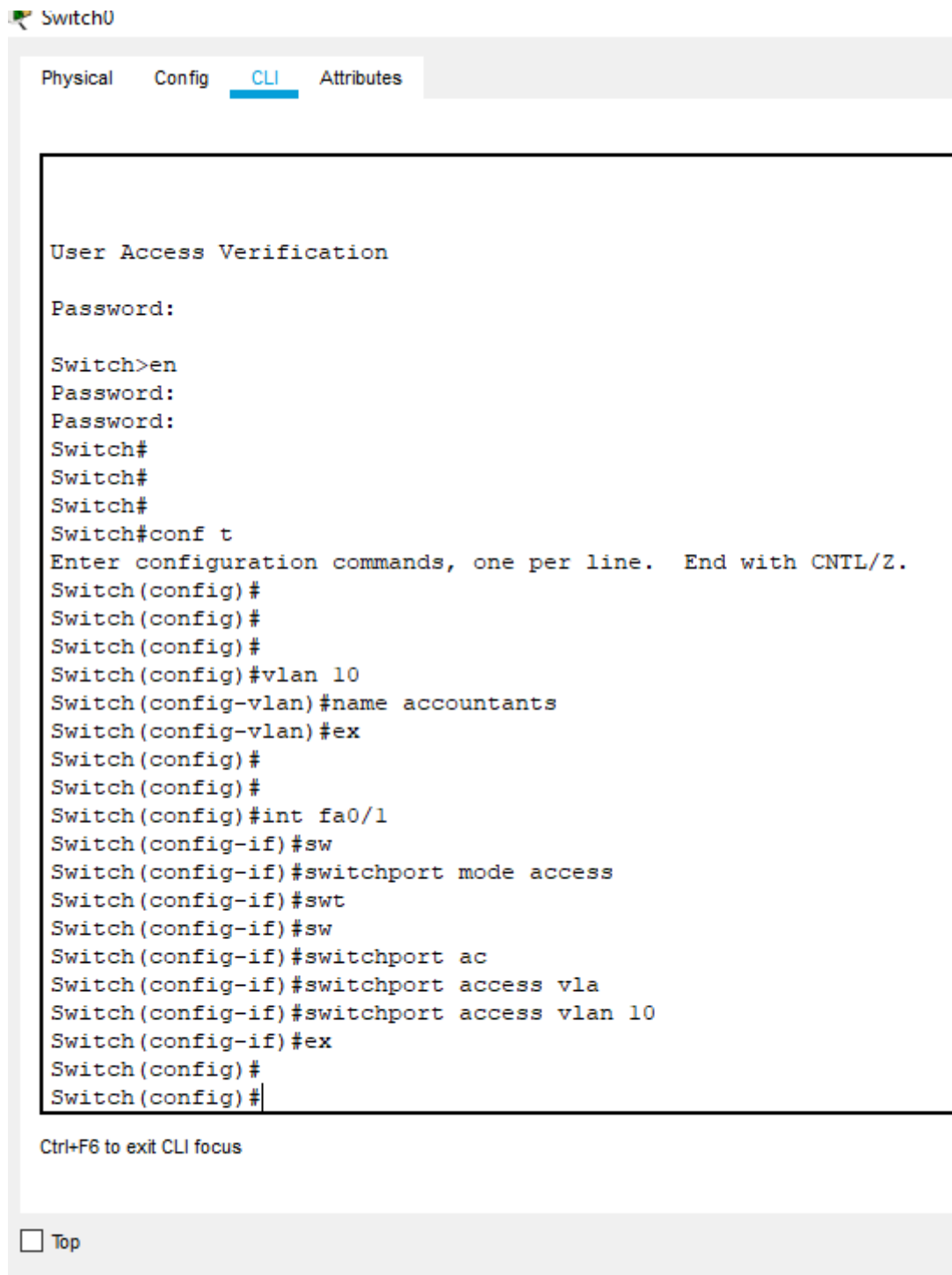
Ctrl+F6 to exit CLI focus

Top

Figure 5.4: Password protection system of Router

5.1.5 Configuration of Basic VLAN:

VLAN configuration is shown in figure 5.5



```
Switch0
Physical  Config  CLI  Attributes

User Access Verification
Password:

Switch>en
Password:
Password:
Switch#
Switch#
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#vlan 10
Switch(config-vlan)#name accountants
Switch(config-vlan)#ex
Switch(config)#
Switch(config)#
Switch(config)#int fa0/1
Switch(config-if)#sw
Switch(config-if)#switchport mode access
Switch(config-if)#swt
Switch(config-if)#sw
Switch(config-if)#switchport ac
Switch(config-if)#switchport access vla
Switch(config-if)#switchport access vlan 10
Switch(config-if)#ex
Switch(config)#
Switch(config)#

Ctrl+F6 to exit CLI focus

 Top
```

Figure 5.5: Configuration of Basic VLAN

5.1.6 Configuration of VTP:

VTP will allow other switches to get all the VLAN from server switch. The configuration is show in figure 5.6

```
Switch13
Switch#
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#
Switch(config)#vtp version 2
Switch(config)#vtp mode server
Device mode already VTP SERVER.
Switch(config)#vtp domain rx
Changing VTP domain name from NULL to rx
Switch(config)#vtp password 1234
Setting device VLAN database password to 1234
Switch(config)#Setting device VLAN database password to 1234
^
% Invalid input detected at '^' marker.

Switch(config)#
Switch(config)#
Switch(config)#
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to up

Switch14
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#vtp version 2
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)#vtp domain rx
Changing VTP domain name from NULL to rx
Switch(config)#vtp password 1234
Setting device VLAN database password to 1234
Switch(config)#Setting device VLAN database password to 1234
^
% Invalid input detected at '^' marker.

Switch(config)#
Switch(config)#
Switch(config)#
```

Figure 5.6: VTP configuration

5.1.7 Configuration of Inter-VLAN in L3 switch:

Configuration of Inter VLAN in L3 switch is shown in figure 5.7

```
multilayer switch
Physical  Config  CLI  Attributes
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#int vlan 1
Switch(config-if)#no ip add
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#ex
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#int vlan 10
Switch(config-if)#ip add 192.168.1.1 255.255.255.0
Switch(config-if)#no sh
Switch(config-if)#ex
Switch(config)#
Switch(config)#
Switch(config)#int vlan 20
Switch(config-if)#ip add 192.168.2.1 255.255.255.0
Switch(config-if)#nosh
Switch(config-if)#
^
% Invalid input detected at '^' marker.

Switch(config-if)#
Switch(config-if)#
Switch(config-if)#no sh
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#ex
Switch(config)#
Switch(config)#ip routing
Switch(config)#
```

Ctrl+F6 to exit CLI focus

Top

Figure 5.7: configuration of Inter VLAN in layer 3 switch

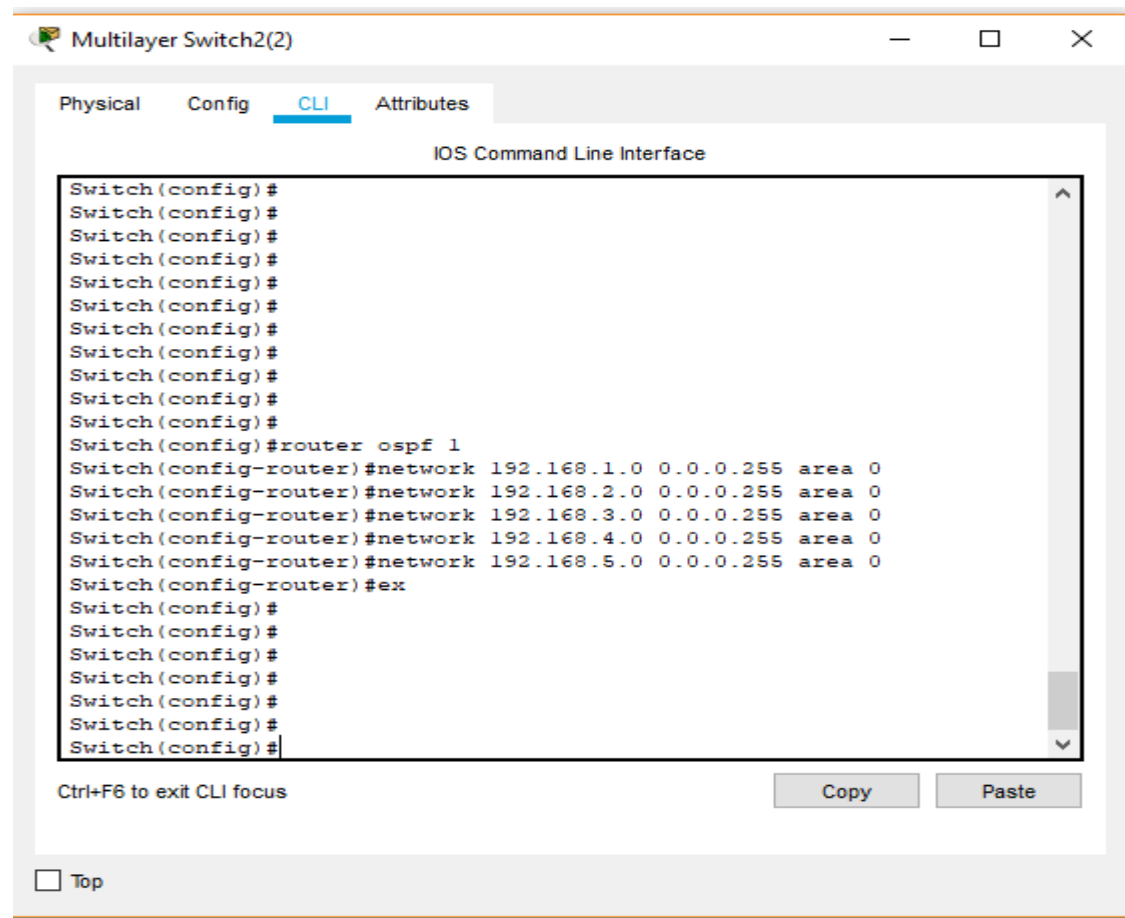
5.1.8 Routing Protocols:

We have use three types of routing protocol.

1. OSPF
2. Static Routing
3. Default Routing

5.1.8.1 Configuration of OSPF Routing protocol:

For configuring OSPF we have to do the following command that is given in figure 5.8



The screenshot shows a window titled "Multilayer Switch2(2)" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following commands and prompts:

```
Switch(config)#  
Switch(config)#  
Switch(config)#  
Switch(config)#  
Switch(config)#  
Switch(config)#  
Switch(config)#  
Switch(config)#  
Switch(config)#  
Switch(config)#  
Switch(config)#  
Switch(config)#  
Switch(config)#router ospf 1  
Switch(config-router)#network 192.168.1.0 0.0.0.255 area 0  
Switch(config-router)#network 192.168.2.0 0.0.0.255 area 0  
Switch(config-router)#network 192.168.3.0 0.0.0.255 area 0  
Switch(config-router)#network 192.168.4.0 0.0.0.255 area 0  
Switch(config-router)#network 192.168.5.0 0.0.0.255 area 0  
Switch(config-router)#ex  
Switch(config)#  
Switch(config)#  
Switch(config)#  
Switch(config)#  
Switch(config)#  
Switch(config)#
```

At the bottom of the window, there is a "Ctrl+F6 to exit CLI focus" message, "Copy" and "Paste" buttons, and a "Top" button.

Figure 5.8: configuration of OSPF Routing protocol

5.1.8.2 Configuration of Static Routing protocol:

Structure of static routing in router is like

< ip route > < destination > <destination mask> <next router address>

```
Router(config)#ip route 192.168.0.0 255.255.0.0 172.16.20.2
```

5.1.8.3 Configuration of Default Routing:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 172.16.20.2
```

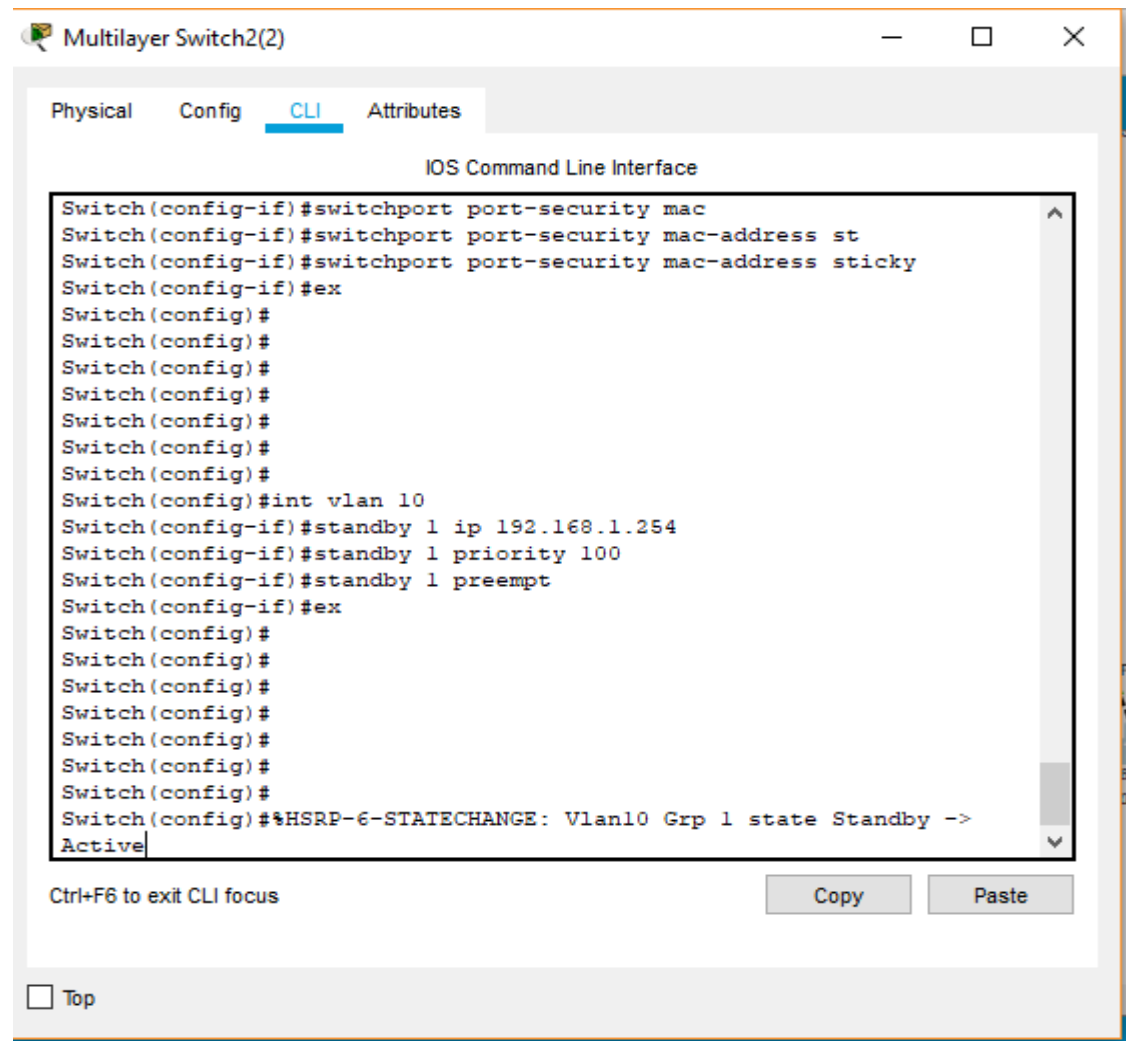
5.1.9 Configuration of Rapid Spanning Tree Protocol (RSTP)

Configuration is like

```
Switch(config)#spanning-tree mode Rapid-pvst
```

5.1.10 Configuration of Hot Standby Routing Protocol (HSRP) in Layer 3 switch

Configuration of HSRP in layer 3 switch is given in the figure 5.9



The screenshot shows a window titled "Multilayer Switch2(2)" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following commands and their results:

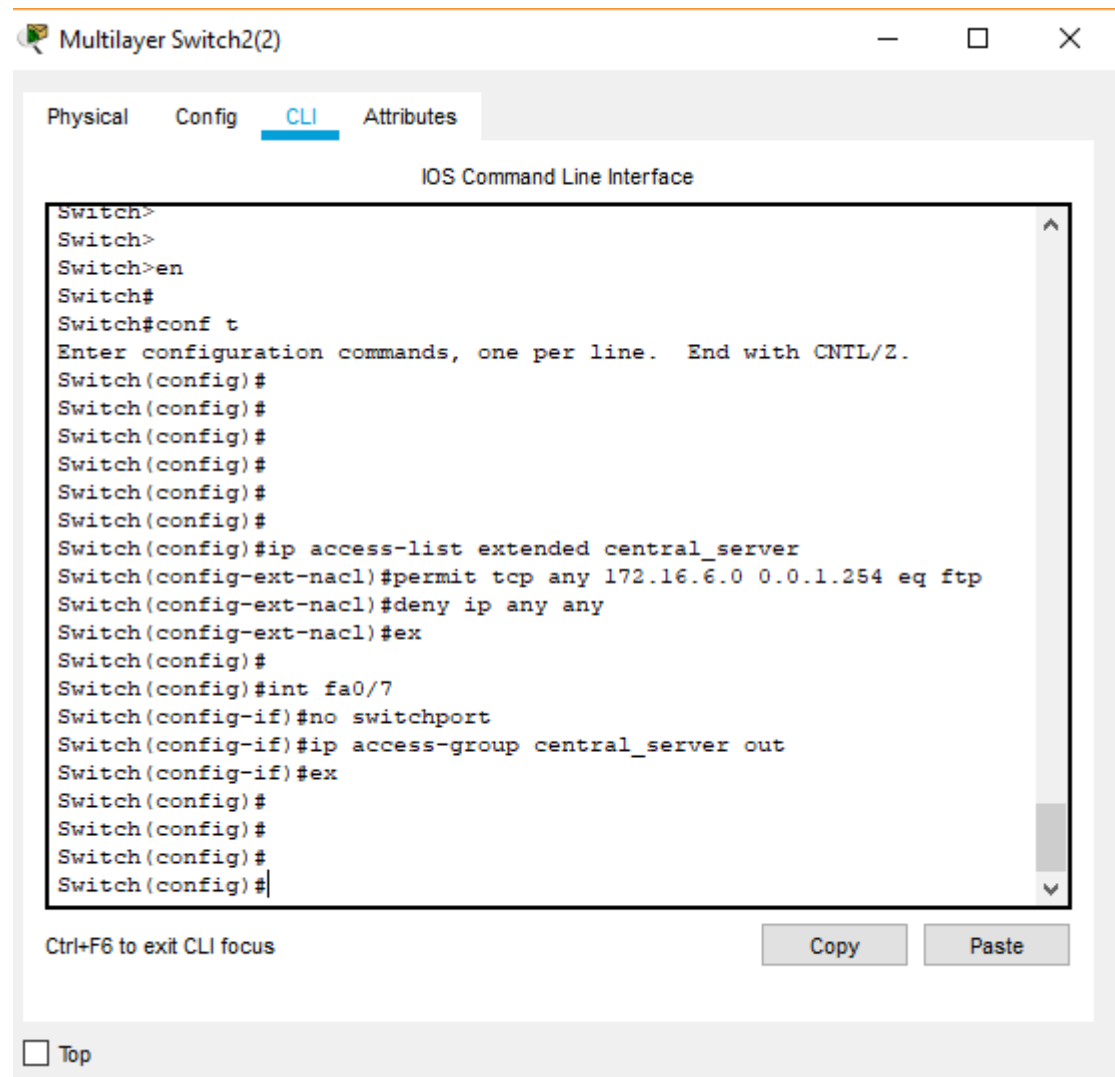
```
Switch(config-if)#switchport port-security mac
Switch(config-if)#switchport port-security mac-address st
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#ex
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#int vlan 10
Switch(config-if)#standby 1 ip 192.168.1.254
Switch(config-if)#standby 1 priority 100
Switch(config-if)#standby 1 preempt
Switch(config-if)#ex
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#%HSRP-6-STATECHANGE: Vlan10 Grp 1 state Standby ->
Active
```

Below the terminal output, there are "Copy" and "Paste" buttons, and a "Top" button with a checkbox.

Figure 5.9: Configuration of HSRP

5.1.11 Configuration of Access Control List (ACL)

Configuration of ACL in a layer 3 switch is shown in figure 5.10



The screenshot shows a window titled "Multilayer Switch2(2)" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following commands and prompts:

```
Switch>
Switch>
Switch>en
Switch#
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#ip access-list extended central_server
Switch(config-ext-nacl)#permit tcp any 172.16.6.0 0.0.1.254 eq ftp
Switch(config-ext-nacl)#deny ip any any
Switch(config-ext-nacl)#ex
Switch(config)#
Switch(config)#int fa0/7
Switch(config-if)#no switchport
Switch(config-if)#ip access-group central_server out
Switch(config-if)#ex
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
```

Below the terminal window, there is a "Ctrl+F6 to exit CLI focus" message and "Copy" and "Paste" buttons. At the bottom left, there is a "Top" button.

Figure 5.10: Configuration of ACL

5.1.12 Configuration of ASA Firewall

The configuration of Firewall is given in figure 5.11 to figure 5.13



```
ASA4
Physical Config CLI Attributes
ciscoasa(config)#
ciscoasa(config)#int vlan 1
ciscoasa(config-if)#name if ins
^
% Invalid input detected at '^' marker.

ciscoasa(config-if)#nameif inside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#ip add 172.16.10.1 255.255.255.0
Interface address is not on same subnet as DHCP pool
ERROR: ip address command failed
ciscoasa(config-if)#ex
ciscoasa(config)#
ciscoasa(config)#int vlan 2
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#ip add 172.16.20.2 255.255.255.0
ciscoasa(config-if)#ex
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#int vlan 3
ciscoasa(config-if)#no
% Incomplete command.
ciscoasa(config-if)#no fo
% Incomplete command.
ciscoasa(config-if)##no forward int
^
% Invalid input detected at '^' marker.

ciscoasa(config-if)#no forward interface vlan 2
ciscoasa(config-if)#na
% Ambiguous command: "na"
ciscoasa(config)#nameif outsidel
^
% Invalid input detected at '^' marker.

ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#int et0/1
```

Ctrl+F6 to exit CLI focus

Top

Figure 5.11: configuration of firewall part 1


```

iscoasa(config)#
iscoasa(config)#
iscoasa(config)#
iscoasa(config)#int et0/1
iscoasa(config-if)#switchport mode access
      ^
Invalid input detected at '^' marker.

iscoasa(config-if)#switchport access vlan 2
iscoasa(config-if)#ex
iscoasa(config)#
iscoasa(config)#int et0/2
iscoasa(config-if)#switchport access vlan 3
iscoasa(config-if)#ex
iscoasa(config)#int et0/0
iscoasa(config-if)#switchport access vlan 1
iscoasa(config-if)#ex
iscoasa(config)#
iscoasa(config)#
iscoasa(config)#int et0/3
iscoasa(config-if)#switchport access vlan 1
iscoasa(config-if)#ex
iscoasa(config)#
iscoasa(config)#object network LAN
iscoasa(config-network-object)#subnet 192.168.0.0 255.255.0.0
iscoasa(config-network-object)#nat (inside,outside) dynamic interface
iscoasa(config-network-object)#ciscoasa(config-network-object)#exit
      ^
Invalid input detected at '^' marker.

iscoasa(config-network-object)#
iscoasa(config-network-object)#
iscoasa(config-network-object)#route inside 192.168.0.0 255.255.0.0 172.16.10.3 1
iscoasa(config)#route inside 172.16.6.0 255.255.254.0 172.16.10.3 1
iscoasa(config)#route inside 192.168.0.0 255.255.0.0 172.16.10.4 1
iscoasa(config)#route outside 0.0.0.0 0.0.0.0 172.16.30.1 1
iscoasa(config)#route outside1 221.221.221.0 255.255.255.0 172.16.20.1 1
LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to down

```

!+F6 to exit CLI focus

Figure 5.12: Configuration of firewall part 2

```
Physical  Config  CLI  Attributes  K
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#int et0/3
ciscoasa(config-if)#switchport access vlan 1
ciscoasa(config-if)#ex
ciscoasa(config)#
ciscoasa(config)#object network LAN
ciscoasa(config-network-object)#subnet 192.168.0.0 255.255.0.0
ciscoasa(config-network-object)#nat (inside,outside) dynamic interface
ciscoasa(config-network-object)#ciscoasa(config-network-object)#exit
^
% Invalid input detected at '^' marker.

ciscoasa(config-network-object)#
ciscoasa(config-network-object)#
ciscoasa(config-network-object)#route inside 192.168.0.0 255.255.0.0 172.16.10.3 1
ciscoasa(config)#route inside 172.16.6.0 255.255.254.0 172.16.10.3 1
ciscoasa(config)#route inside 192.168.0.0 255.255.0.0 172.16.10.4 1
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 172.16.30.1 1
ciscoasa(config)#route outside1 221.221.221.0 255.255.255.0 172.16.20.1 1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to down

^
% Invalid input detected at '^' marker.

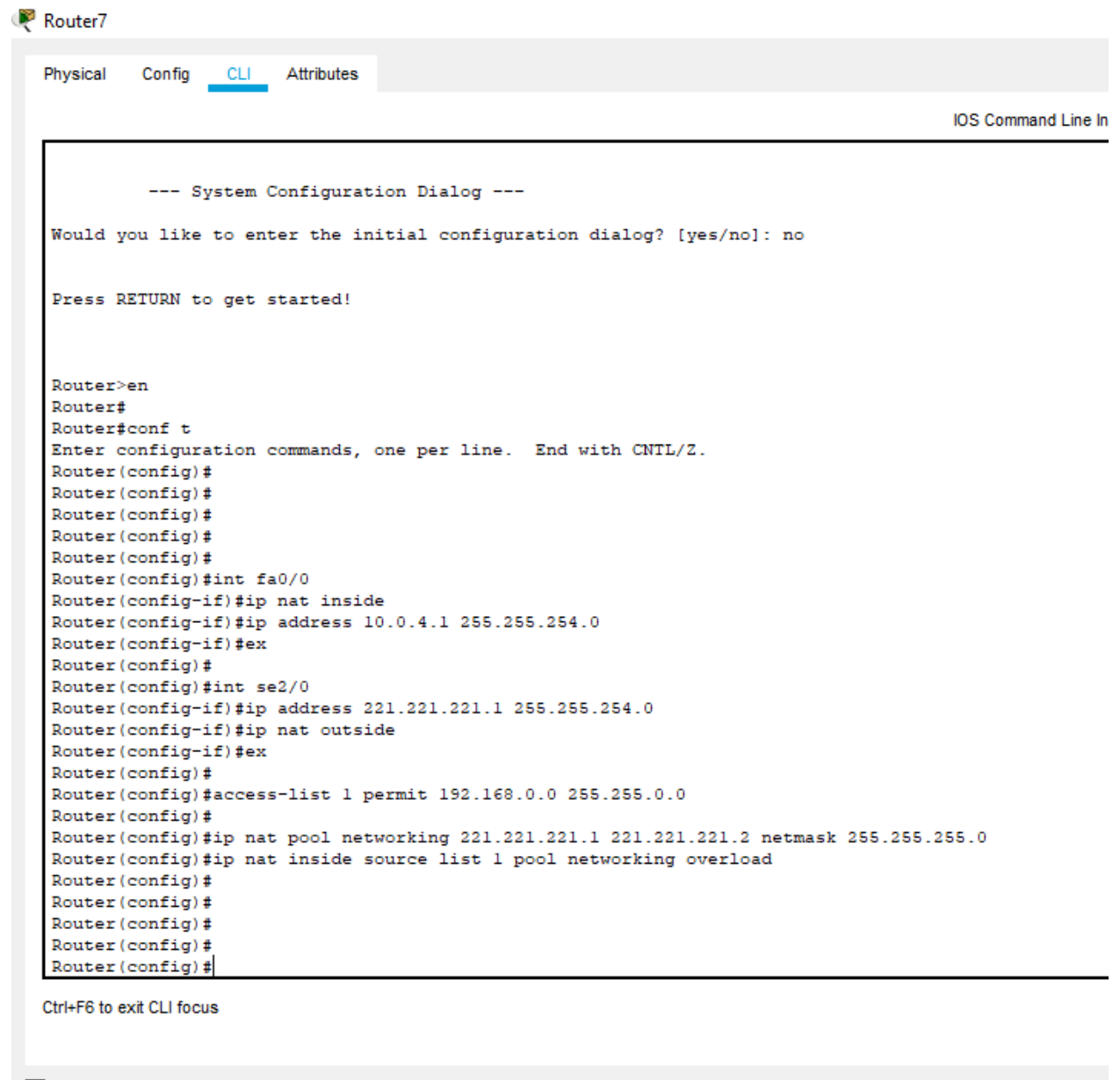
ciscoasa(config)#class-map inspection_Default
ciscoasa(config-cmap)#match default-inspection-traffic
ciscoasa(config-cmap)#ex
ciscoasa(config)#
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_Default
ciscoasa(config-pmap-c)#inspect icmp
ciscoasa(config-pmap-c)#ex
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
```

Ctrl+F6 to exit CLI focus

Figure 5.13: Configuration of firewall part 3

5.1.13 Configuration of PAT:

We have shown the configuration of PAT in the figure 5.14



```
Router7
Physical Config CLI Attributes
IOS Command Line In

--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!

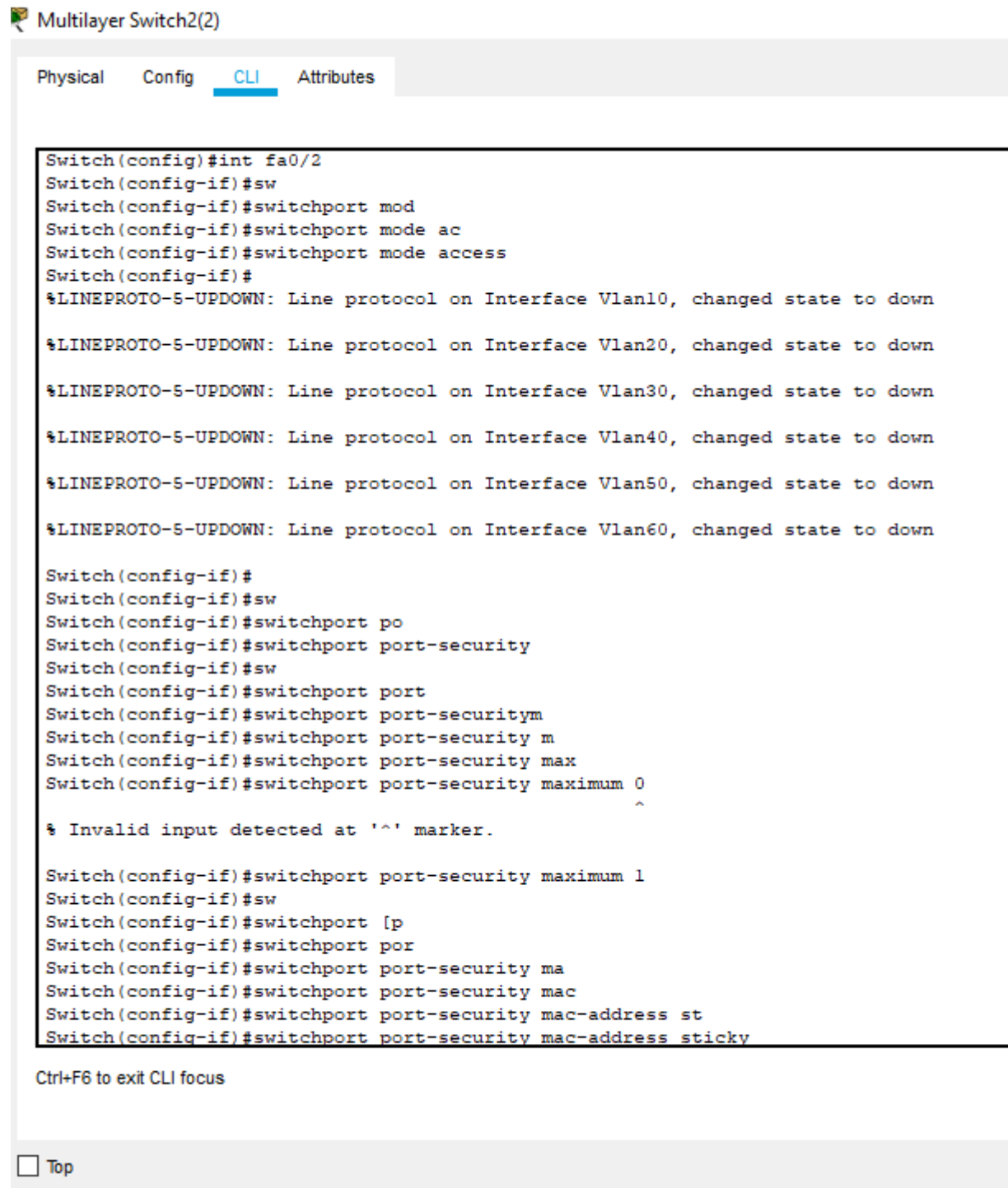
Router>en
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#ip address 10.0.4.1 255.255.254.0
Router(config-if)#ex
Router(config)#
Router(config)#int se2/0
Router(config-if)#ip address 221.221.221.1 255.255.254.0
Router(config-if)#ip nat outside
Router(config-if)#ex
Router(config)#
Router(config)#access-list 1 permit 192.168.0.0 255.255.0.0
Router(config)#
Router(config)#ip nat pool networking 221.221.221.1 221.221.221.2 netmask 255.255.255.0
Router(config)#ip nat inside source list 1 pool networking overload
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
```

Ctrl+F6 to exit CLI focus

Figure 5.14: Configuration of PAT

5.1.14 Configuration of Port security:

The Configuration of port security is given in figure 5.15



Multilayer Switch2(2)

Physical Config **CLI** Attributes

```
Switch(config)#int fa0/2
Switch(config-if)#sw
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode ac
Switch(config-if)#switchport mode access
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan50, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan60, changed state to down

Switch(config-if)#
Switch(config-if)#sw
Switch(config-if)#switchport po
Switch(config-if)#switchport port-security
Switch(config-if)#sw
Switch(config-if)#switchport port
Switch(config-if)#switchport port-securitym
Switch(config-if)#switchport port-security m
Switch(config-if)#switchport port-security max
Switch(config-if)#switchport port-security maximum 0
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#sw
Switch(config-if)#switchport [p
Switch(config-if)#switchport por
Switch(config-if)#switchport port-security ma
Switch(config-if)#switchport port-security mac
Switch(config-if)#switchport port-security mac-address st
Switch(config-if)#switchport port-security mac-address sticky
```

Ctrl+F6 to exit CLI focus

Top

Figure 5.15: Configuration of Port security

5.1.15 Configuration of VPN

Configuration of Virtual Private Network in a single 1941 Router is given in figure 5.16

```
Router8
Physical Config CLI Attributes
IOS Command Line Interface
Router(config)#
Router(config)#
Router(config)#interface se0/0/0
Router(config-if)#ip address 220.220.220.2 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#ip route 0.0.0.0 0.0.0.0 220.220.220.1
Router(config)#
Router(config)#crypto isakmp policy 10
Router(config-isakmp)# encryption aes 256
Router(config-isakmp)# authentication pre-share
Router(config-isakmp)# group 5
Router(config-isakmp)#crypto isakmp key secretkey address 200.200.200.1
Router(config)#crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac
Router(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router(config-crypto-map)# set peer 200.200.200.1
Router(config-crypto-map)# set pfs group5
Router(config-crypto-map)# set security-association lifetime seconds 86400
Router(config-crypto-map)# set transform-set R1-R3
Router(config-crypto-map)# match address 100
Router(config-crypto-map)#
Router(config-crypto-map)#exit
Router(config)#
Router(config)#
Router(config)#interface GigabitEthernet0/0
Router(config-if)# crypto map IPSEC-MAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#
Router(config-if)#access-list 100 permit ip 172.30.0.0 0.0.255.255 192.168.0.0 0.0.255.255
Router(config)#
Router(config)#access-list 100 permit ip 10.0.0.0 0.0.1.255 192.168.0.0 0.0.255.255
Router(config)#
Ctrl+F6 to exit CLI focus
Top
```

Figure 5.16: Configuration of VPN

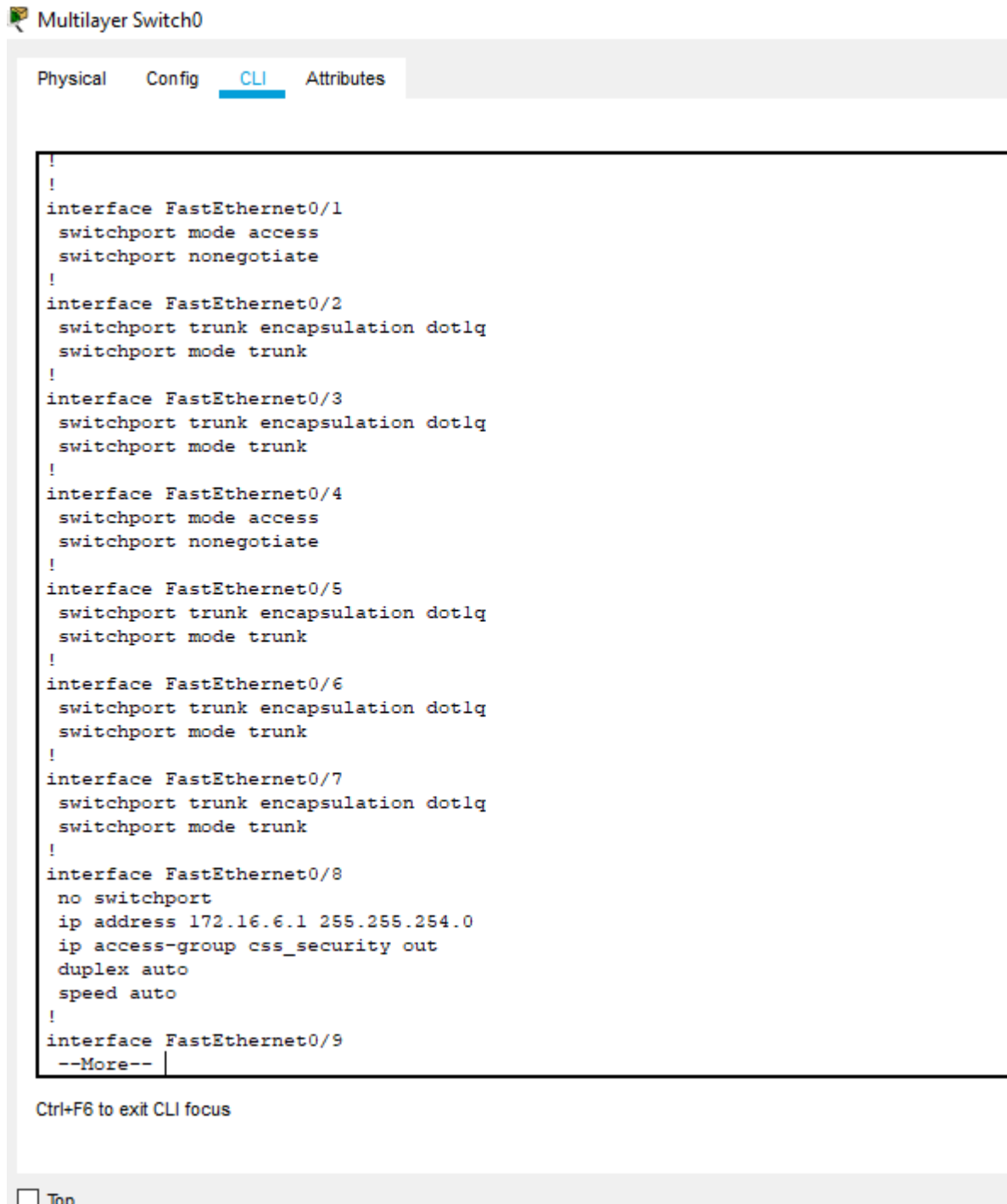


Figure 5.18: Running configuration of Switch part 2

Physical Config **CLI** Attributes

```

!
interface Vlan1
 ip address 172.16.10.3 255.255.255.0
!
interface Vlan10
 mac-address 000d.bde8.3401
 ip address 192.168.1.1 255.255.255.0
 ip access-group 110 in
 standby 1 ip 192.168.1.254
 standby 1 priority 150
 standby 1 preempt
!
interface Vlan20
 mac-address 000d.bde8.3402
 ip address 192.168.2.1 255.255.255.0
 ip access-group 120 in
 standby 1 ip 192.168.2.254
 standby 1 priority 150
 standby 1 preempt
!
interface Vlan30
 mac-address 000d.bde8.3403
 ip address 192.168.3.1 255.255.255.0
 ip access-group 130 in
 standby 1 ip 192.168.3.254
 standby 1 priority 150
 standby 1 preempt
!
interface Vlan40
 mac-address 000d.bde8.3404
 ip address 192.168.4.1 255.255.255.0
 ip access-group 140 in
 standby 1 ip 192.168.4.254
 standby 1 priority 150
 standby 1 preempt
!
interface Vlan50
 mac-address 000d.bde8.3405
--More--

```

Ctrl+F6 to exit CLI focus

Top

Figure 5.19: Running configuration of Switch part 3

Physical Config **CLI** Attributes

```
!
interface Vlan50
  mac-address 000d.bde8.3405
  ip address 192.168.5.1 255.255.255.0
  ip access-group 150 in
  standby 1 ip 192.168.5.254
  standby 1 priority 150
  standby 1 preempt
!
interface Vlan60
  mac-address 000d.bde8.3406
  ip address 192.168.6.1 255.255.255.0
  ip access-group 160 in
  standby 1 ip 192.168.6.254
  standby 1 priority 150
  standby 1 preempt
!
interface Vlan99
  mac-address 000d.bde8.3407
  no ip address
!
router ospf 1
  log-adjacency-changes
  network 192.168.1.0 0.0.0.255 area 0
  network 192.168.2.0 0.0.0.255 area 0
  network 192.168.3.0 0.0.0.255 area 0
  network 192.168.4.0 0.0.0.255 area 0
  network 192.168.5.0 0.0.0.255 area 0
  network 192.168.6.0 0.0.0.255 area 0
  network 172.16.2.0 0.0.1.255 area 0
  network 172.16.6.0 0.0.1.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.10.2 2
ip route 0.0.0.0 0.0.0.0 172.16.10.1
!
ip flow-export version 9
!
--More--
```

Ctrl+F6 to exit CLI focus

Top

Figure 5.20: Running configuration of Switch part 4

Multi-layer Switch

Physical Config **CLI** Attributes

```
network 172.16.2.0 0.0.1.255 area 0
network 172.16.6.0 0.0.1.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.10.2 2
ip route 0.0.0.0 0.0.0.0 172.16.10.1
!
ip flow-export version 9
!
!
ip access-list extended css_security
 permit tcp any host 172.16.6.10 eq ftp
 permit tcp 192.168.5.0 0.0.0.255 host 172.16.6.10 eq telnet
 deny ip any 172.16.6.0 0.0.1.255
!
no cdp run
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
!
end

Switch#
Switch#
Switch#
Switch#
```

Ctrl+F6 to exit CLI focus

Figure 5.21: Running configuration of Switch part 5

5.2.2 Checking the Routing:

We have shown the checking process of routing configuration in figure 5.22

```
router
Physical Config CLI Attributes
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 200.200.200.2 to network 0.0.0.0

    172.16.0.0/16 is variably subnetted, 6 subnets, 3 masks
S       172.16.6.0/23 [1/0] via 172.16.30.2
        [1/0] via 172.16.50.2
S       172.16.8.0/23 [1/0] via 172.16.30.2
        [1/0] via 172.16.50.2
C       172.16.30.0/24 is directly connected, GigabitEthernet0/0
L       172.16.30.1/32 is directly connected, GigabitEthernet0/0
C       172.16.50.0/24 is directly connected, GigabitEthernet0/1
L       172.16.50.1/32 is directly connected, GigabitEthernet0/1
S       192.168.0.0/16 [1/0] via 172.16.30.2
    200.200.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.200.200.0/24 is directly connected, Serial0/1/0
L       200.200.200.1/32 is directly connected, Serial0/1/0
S*      0.0.0.0/0 [1/0] via 200.200.200.2

Router#
Router#
Router#
Router#
Router#
```

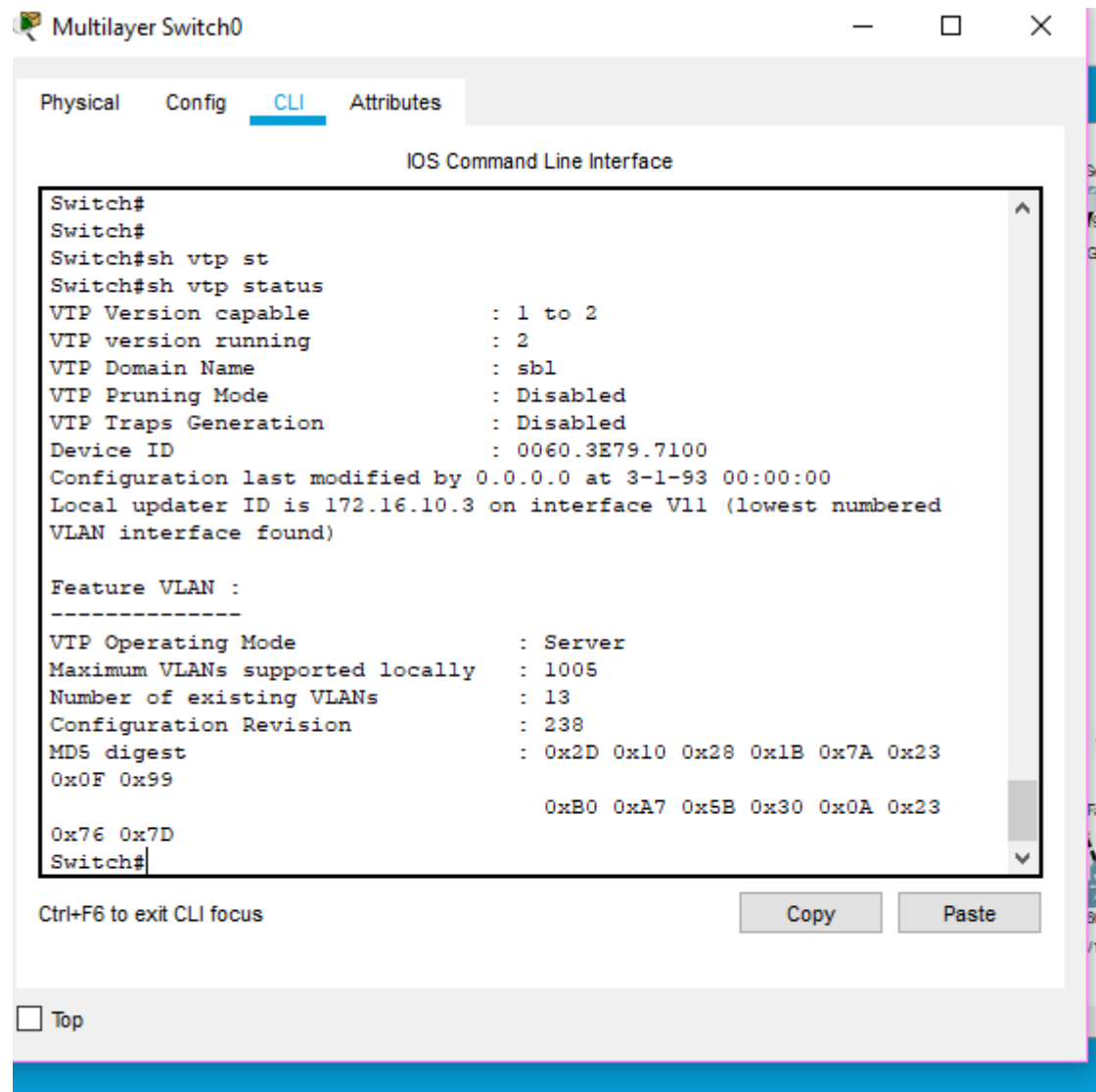
Ctrl+F6 to exit CLI focus

Top

Figure 5.22: Checking the routing configuration

5.2.3 Checking the VTP

Show VTP status will display the VTP status of a switch. Figure 5.23 show us the phenomena



The screenshot shows a window titled "Multilayer Switch0" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following commands and their results:

```
Switch#
Switch#
Switch#sh vtp st
Switch#sh vtp status
VTP Version capable      : 1 to 2
VTP version running     : 2
VTP Domain Name         : sb1
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID                : 0060.3E79.7100
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 172.16.10.3 on interface V11 (lowest numbered
VLAN interface found)

Feature VLAN :
-----
VTP Operating Mode      : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 13
Configuration Revision  : 238
MD5 digest              : 0x2D 0x10 0x28 0x1B 0x7A 0x23
                        0x0F 0x99
                        0xB0 0xA7 0x5B 0x30 0x0A 0x23
                        0x76 0x7D
Switch#
```

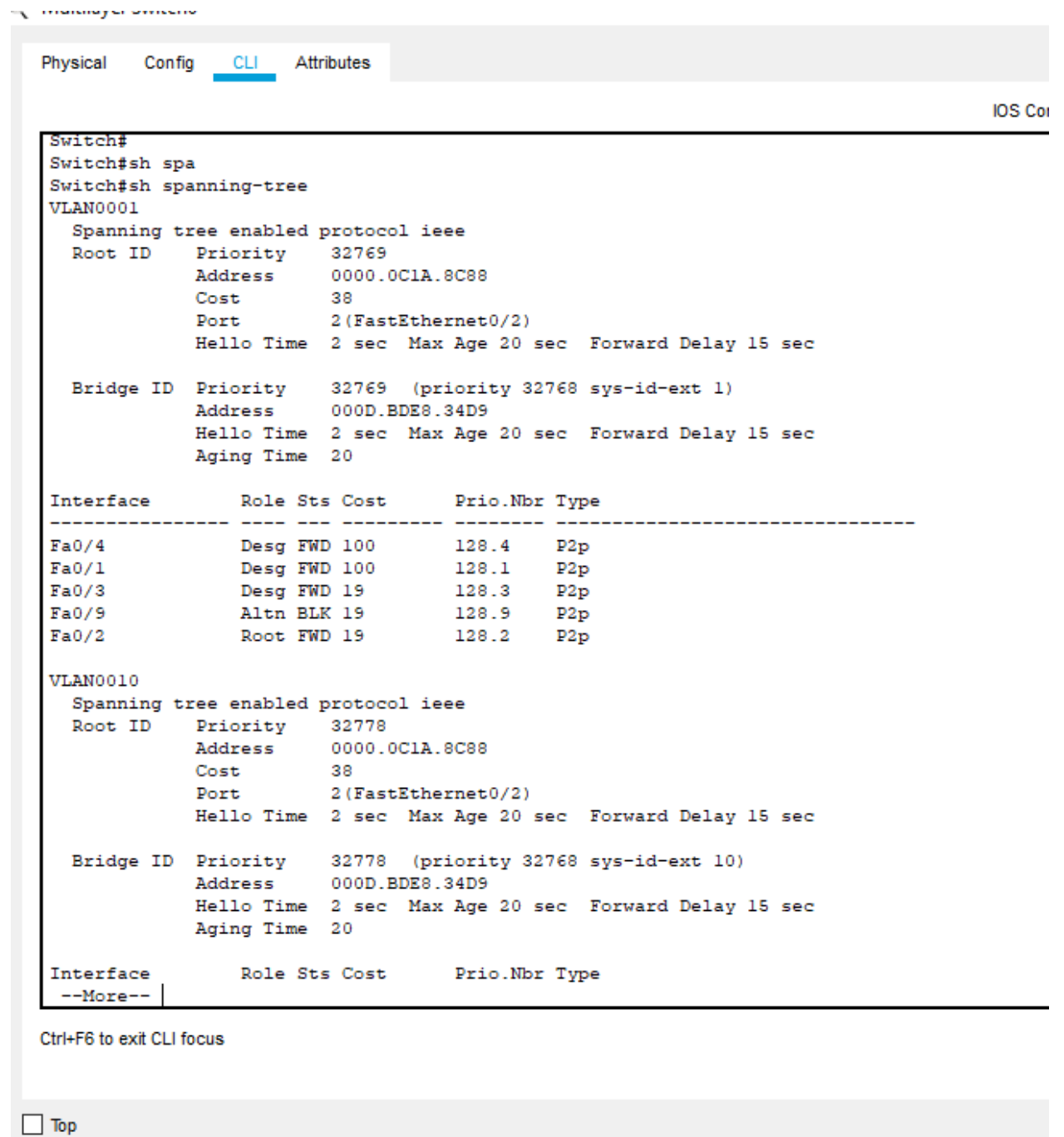
Below the terminal output, there are buttons for "Copy" and "Paste", and a "Top" button with a checkbox.

Figure 5.23: Checking the VTP configuration

5.2.4 Checking the RSTP

Show spanning-tree will show all the information about spanning tree. Figure 5.24

shows us that



```
Switch#
Switch#sh spa
Switch#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
            Address    0000.0C1A.8C88
            Cost      38
            Port      2 (FastEthernet0/2)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
            Address    000D.BDE8.34D9
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 20

Interface    Role Sts Cost      Prio.Nbr Type
-----
Fa0/4        Desg FWD 100      128.4    P2p
Fa0/1        Desg FWD 100      128.1    P2p
Fa0/3        Desg FWD 19       128.3    P2p
Fa0/9        Altn BLK 19       128.9    P2p
Fa0/2        Root FWD 19       128.2    P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
            Address    0000.0C1A.8C88
            Cost      38
            Port      2 (FastEthernet0/2)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778 (priority 32768 sys-id-ext 10)
            Address    000D.BDE8.34D9
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 20

Interface    Role Sts Cost      Prio.Nbr Type
--More--
```

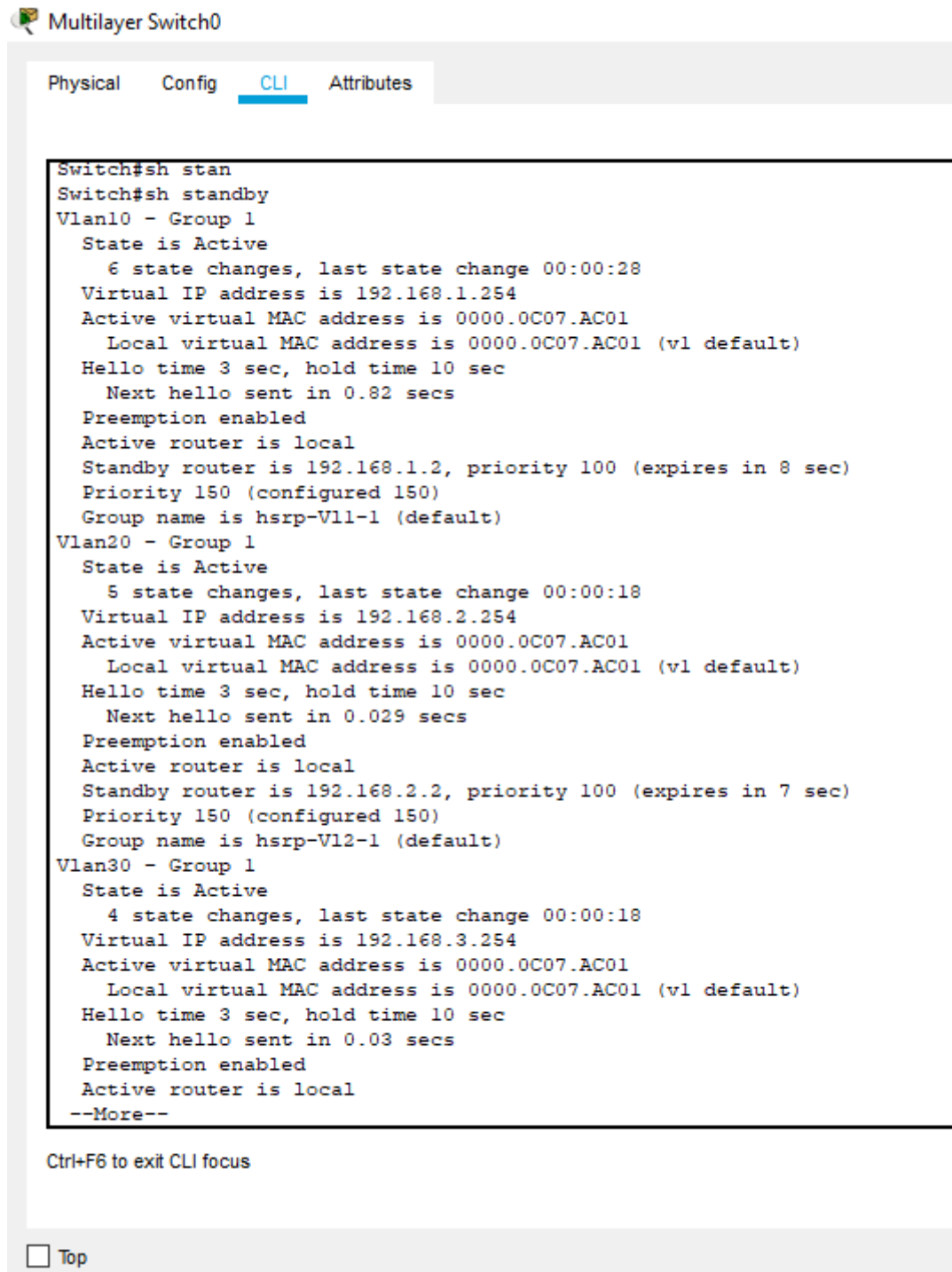
Ctrl+F6 to exit CLI focus

Top

Figure 5.24: Checking the RSTP configuration

5.2.5 Checking the HSRP:

Show standby will show information about the HSRP. We can see that in figure 5.25



Multilayer Switch0

Physical Config **CLI** Attributes

```
Switch#sh stan
Switch#sh standby
Vlan10 - Group 1
  State is Active
    6 state changes, last state change 00:00:28
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (vl default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.82 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.2, priority 100 (expires in 8 sec)
  Priority 150 (configured 150)
  Group name is hsrp-Vl1-1 (default)
Vlan20 - Group 1
  State is Active
    5 state changes, last state change 00:00:18
  Virtual IP address is 192.168.2.254
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (vl default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.029 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.2.2, priority 100 (expires in 7 sec)
  Priority 150 (configured 150)
  Group name is hsrp-Vl2-1 (default)
Vlan30 - Group 1
  State is Active
    4 state changes, last state change 00:00:18
  Virtual IP address is 192.168.3.254
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (vl default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.03 secs
  Preemption enabled
  Active router is local
--More--

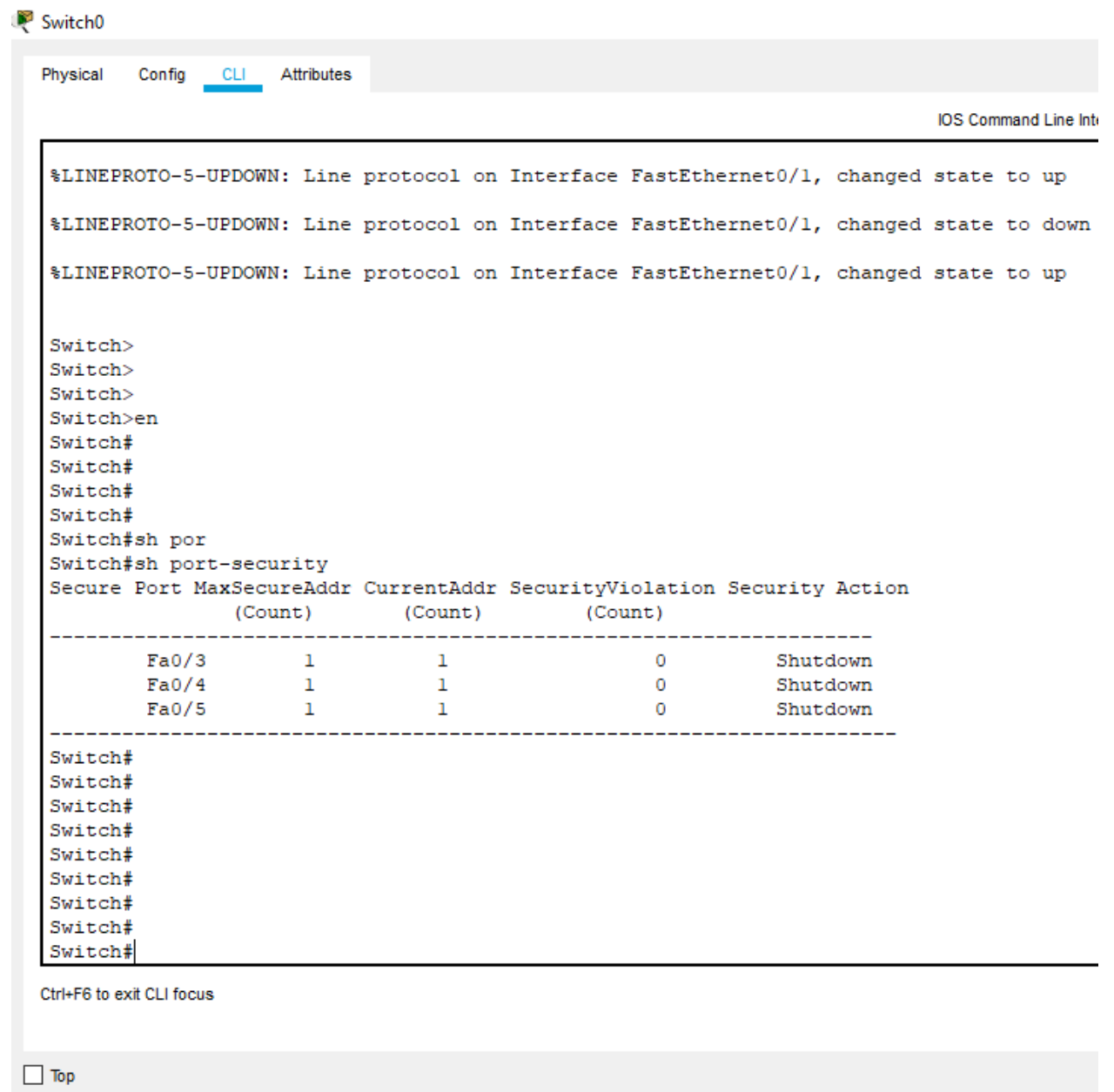
Ctrl+F6 to exit CLI focus
```

Top

Figure 5.25: Checking the HSRP configuration

5.2.6 Checking port security

For checking the port security we have to enter the command that is given in figure 5.26



The screenshot shows a network switch CLI interface for 'Switch0'. The interface has tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' selected. The title bar indicates 'IOS Command Line Interface'. The CLI session shows the following commands and output:

```
Switch0
Physical Config CLI Attributes
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch>
Switch>
Switch>
Switch>en
Switch#
Switch#
Switch#
Switch#
Switch#sh por
Switch#sh port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)          (Count)          (Count)
-----
          Fa0/3            1            1            0            Shutdown
          Fa0/4            1            1            0            Shutdown
          Fa0/5            1            1            0            Shutdown
-----

Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
```

Below the CLI window, there is a 'Ctrl+F6 to exit CLI focus' message and a 'Top' button.

Figure 5.26: Checking the Port security

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

Establishing Security and maintaining it is a very difficult Task. Our project can ensure the structural and topological security. We have tried to provide security with the available devices with their built in configuration, without using any kind of additional software. And the security methods that we have used Like ACL, VPN, port security, Secured Shell (SSH), Console passwords are the modern technologies to provide network security. But our project has some limitations

6.1 Limitation of our project

1. Packet tracer provided very less functionalities for Cisco ASA firewall. And most of the time firewall act a little bit weird. For a problem free firewall we have to use GNS3 simulator. But collecting and installing IOS of devices is very lengthy and costly task.
2. VTP, HSRP, RPVST, port security only supports in Cisco switches or routers.
3. Software based threats can't be detected by our Design. For this you have to use Additional software or distribution of Linux

6.2 Scope for Further Developments

As after implementing our project in packet tracer, we found less functions for firewall, so we will implement this topology in GSN3 with **IPV6** in very near future. If any better technology for securing network structure, appear in future then we will update our project too. And we will try to implement this topology in any new corporate office.

REFERENCES

- [1] VLAN From:
<http://etutorials.org/Networking/Lan+switching+first-step/Chapter+8.+Virtual+LANs+VLANs/VLAN+Overview/> [Last accessed on 11 December 2018]
- [2] ACL Apply. Available from :
<http://www.networkstraining.com/ccna-training-access-control-lists/> [Last Accessed on 12 January 2019]
- [3] Firewall from:
<https://personalfirewall.comodo.com/what-is-firewall.html> [Last accessed on 29 January 2019]
- [4] Remote access VPN. From:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/vpnrmote.html [Last Accessed on 22February 2019]
- [5] Cisco IOS. Available from:
http://kfo.ath.cx/windowmaker/2012_windowmaker.info/wiki/Cisco_IOS
[Last Accessed 22 on December 2018]
- [7] Cisco Packet Tracer.
From:<https://studylib.net/doc/7797209/packet-tracer-%E2%80%93-creating-a-new-topology-what-is-packet-tracer> [Last accessed on 10 December 2018]
- [8] Troubleshooting From:
<http://www.ciscopress.com/articles/article.asp?p=2180209&seqNum=8>
[Last Accessed on 10 February 2019]

Here is the plagiarism testing report

