

IMPROVING COMPUTER NETWORK SECURITY

BY

POBITRA CHANDRA PAUL

ID: 191-15-12253

SHUBHASISH BHADRA

ID: 191-15-12215

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

Supervised By

Mr. Gazi Zahirul Islam

Assistant Professor

Department of CSE

Daffodil International University

Co-Supervised By

Ms. Nusrat Jahan

Sr. Lecturer

Department of CSE

Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

JANUARY 2022

APPROVAL

This Project titled “**IMPROVING COMPUTER NETWORK SECURITY**”, submitted by **Pobitra Chandra Paul**, Id No: **191-15-12253** and **Shubhasish Bhadra**, Id No: **191-15-12215** 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 **02 January 2022**.

BOARD OF EXAMINERS



Dr. Touhid Bhuiyan

Professor and Head

Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Chairman

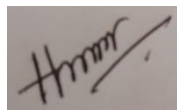


Moushumi Zaman Bonny

Assistant Professor

Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Md. Mahfujur Rahman

Senior Lecturer

Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Dr. Md Arshad Ali

Associate Professor

Department of Computer Science and Engineering
Hajee Mohammad Danesh Science and Technology University

External Examiner

DECLARATION

We hereby declare that, this project has been done by us under the supervision of Mr. Gazi Zahirul Islam, Assistant Professor of Department of Computer Science and Engineering 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 or diploma.

Supervised by:



Mr. Gazi Zahirul Islam

Assistant Professor
Department of Computer Science and Engineering
Daffodil International University

Co-Supervised by:



Ms. Nusrat Jahan

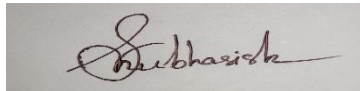
Sr. Lecturer
Department of Computer Science and Engineering
Daffodil International University

Submitted by:



Pobitra Chandra Paul

ID: -191-15-12253
Department of Computer Science and Engineering
Daffodil International University



Shubhasish Bhadra

Id: 191-15-12215
Department of Computer Science and Engineering
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 really grateful and wish our profound our indebtedness to **Mr. Gazi Zahirul Islam** Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of “Networking” to carry out this project. His endless patience ,scholarly guidance ,continual encouragement ,constant and energetic supervision, constructive criticism , valuable advice ,reading many inferior draft and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to **Prof. Dr. Touhid Bhuiyan, 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

Computer network security is a great convenience for users. Network security problem generally includes network system security and data security. Specifically, it refers to the reliability of network system, confidentiality, integrity and availability of data information in the system. This project Title “Improving Computer Network Security” is a communication system head office and branch office. Firewall, Access Control list (ACL) and Virtual Private Network (VPN) are the most popular network security method. SSH has also been configured to enter the router remotely. For this project more secure & realistic we use Network Address Translation (NAT) and Port Address Translation (PAT).

TABLE OF CONTENTS

CONTENTS	PAGE
Board of examiners	i
Declaration	ii
Acknowledgement	iii
Abstract	iv
CHAPTER 1: INTRODUCTION	01-02
1.1 Introduction	01
1.2 Motivation	01
1.3 Objectives	01
1.4 Expected Outcomes	02
CHAPTER 2: BACKGROUND	03-04
2.1 Comparative Analysis	03
2.2 Scope of the Problem	03
2.3 Challenges	04
CHAPTER 3: REQUIREMENT SPECIFICATION	05-14
3.1 Introduction	05
3.2 VLAN	06
3.3 Inter VLAN	07
3.4 DHCP	08
3.5 OSPF Routing protocol	09
3.6 ACL	10
3.7 SSH	10
3.8 NAT	11
3.9 HSRP	12
3.10 Firewall	13
3.11 Port security	14

CHAPTER 4: DESIGN SPECIFICATION	15-19
4.1 Front-end Design	15
4.2 Back-end Design	16
4.3 Implementation Requirements	16
4.4 Simulator	17
4.5 GUI of Packet Tracer	17
CHAPTER 5: IMPLEMENTATION AND TESTING	20-32
5.1 Implementation	20
Assigning IP address into a router's port	20
Password protection system of router	21
Assigning IP address into the pc from DHCP	22
Password protection system of switch	23
Configured VLAN	24
Configuration of Inter-VLAN	25
Configuration of Port security	26
Configuration of OSPF Routing protocol	27
Configuration of Access Control List (ACL)	28
Configuration of ASA Firewall	29
Configuration SSH	30
5.2 Testing Implementation	31
Ping the packet transfer	31
Checking the Routing:	32
CHAPTER 7: CONCLUSION AND FUTURE SCOPE	33-33
7.1 Discussion and Conclusion	33
7.2 Scope for Further Developments	33
REFERENCES	34-35

CHAPTER 1

INTRODUCTION

1.1 Introduction:

When we say the world is security we think such a situation when security is a must. Rising using network, there is a question has come about security ahead continuously. Now, the increase of any network is security. Though there was no importance of the security of network in the past, at present there is a great importance of the implementation of each and every network design. Everyone wants a secured network system. Because network is for trade and business. If there is no security of trade business, nobody will use network.

1.2 Motivation:

Given the large range of current pc and network security attacks, students see a need to strengthen the security of computer system, their own particular-

- Finding suppliers.
- Understanding market opportunities.
- Getting new ideas and innovations.
- Finding inspiration.
- Improving my communication.

1.3 Objectives:

Computer Network security or Data security, access, authentication and authorization becomes important topics in today's context. Every new day, new security threats are coming up and system administrators have to race ahead of these threats to stay up in the game.

Confidentiality: No one can read our data.

Integrity: No one can alter our data.

No notation of authority (signature)

Availability: Network resources available to us when we want (further, not available to unauthorized users).

1.4 Expected Outcomes:

- Define some of the factors driving the need for network security.
- Identify and classify specific examples of attacks.
- Define the terms vulnerability, threat and attack.
- Identify physical points of vulnerability in simple networks.
- Compare and contrast symmetric and asymmetric encryption systems and their vulnerability to attack, and explain the characteristics of hybrid systems.

CHAPTER 2

BACKGROUND STUDY

2.1 Comparative Analysis:

Information technology is the strong strength of present economy, but the information is not always secured and some steps should be taken to get security properly. 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), Port Address Translation (PAT), Virtual Local Area Network (VLAN), Inter VLAN, Virtual Private Network (VPN), Open Shortest Path First (OSPF), Rapid Spanning Tree Protocol (RSTP), Firewall etc. We are trying ensure a more secures network in any organizations.

2.2 Scope of problem:

Computer network security is an important issue in the world. Because, if there is a weakness in the network, the hacker can take away his access. It can then use that access to send malware to all devices connected to the network. In other words all the devices are damaged due to a small error in the network. If we can ensure network own LAN secure our LAN hacking potential will be greatly reduced. In real life everyone is just really worried about their virtual safety. That's why they use a lot of additional software. Sometimes this software can create backdoors and allow hackers to enter. We have tried to make sure both virtual, physical and topological security without using any optional software hence, we used the default security system of network devices. It is a matter of regret that someone considers the system as 100% secured. But it is true that there is no 100% security in network system. So, we are trying to harden the security to make the system difficult to hack.

2.3 Challenges:

There is a security reason when it comes to computer. It is a principal in computer network and a considerable task for network security specialist as it entails defending networks against different cyber assaults, preventing unauthorized user from entering and entrance the system and making sure network integrity. All of these security challenges grow in proportion to the size of the network the largest the network the greater the danger of security difficulties.

CHAPTER 3

REQUIREMENT SPECIFICATION

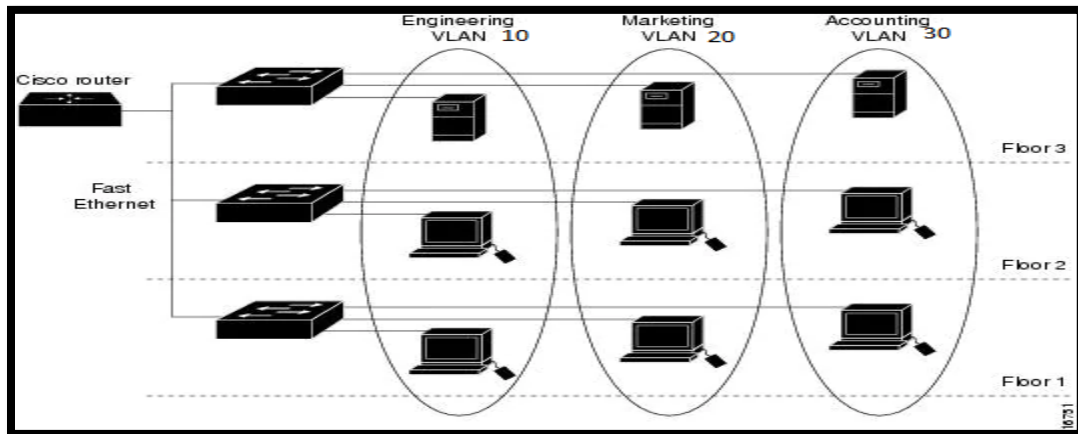
3.1 INTRODUCTION:

This chapter deals with requirement specification.

- VLAN
- Inter- VLAN
- DHCP
- OSPF
- ACL
- SSH
- NAT
- Firewall
- Port Security

3.2 VLAN:

VLAN is a custom network which is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network

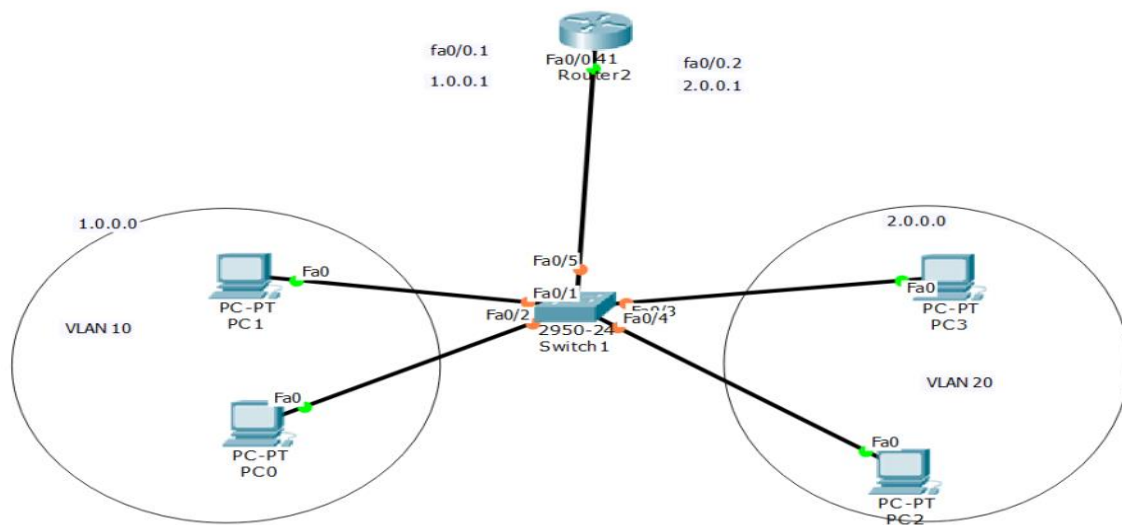


Why have we used VLAN in our network system?

Part of a network helps of rise security, reliability and representation of a network. There are a different of paths a VLAN can be used to fit an institution's needs. One famous use of a VLAN is to personal guest traffic from admin traffic through difference of the network. This permits guest users to access the internet without being on the same network elements.

3.3 Inter-VLAN:

Usually only computers of the same VLAN can communicate between them on a VLAN base network. Can't communicate with other VLAN network. And for this inter VLAN is needed to communicate with other VLAN network.

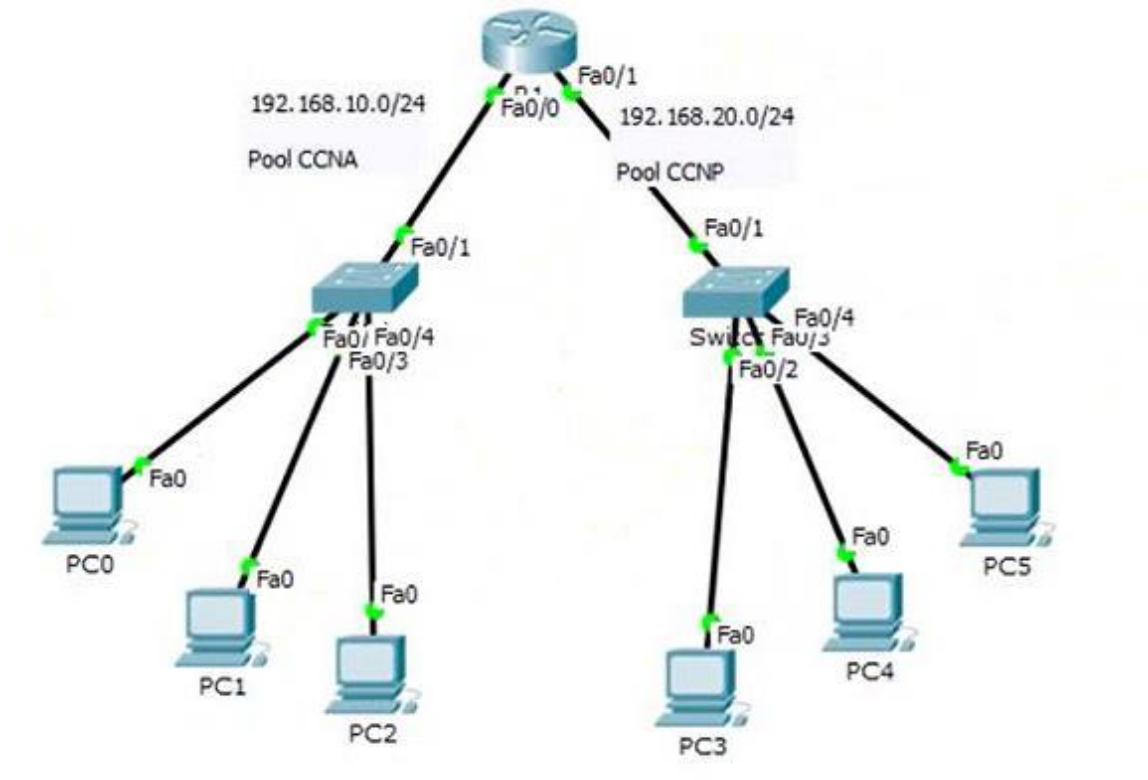


Why have we used Inter-VLAN in our network system?

The purpose of inter-VLAN is to exchange data with each VLAN in the network.

3.4 DHCP:

DHCP Server is a network server. The Dynamic Host Configuration Protocol, or DHCP function, is used to perform the IP configuration of hosts on TCP / IP networks. It's automatically provides and assign IP address. DHCP can be configured in two place, Router and Server.



How DHCP server works?

DHCP connection establish by DHCP client and DHCP server.

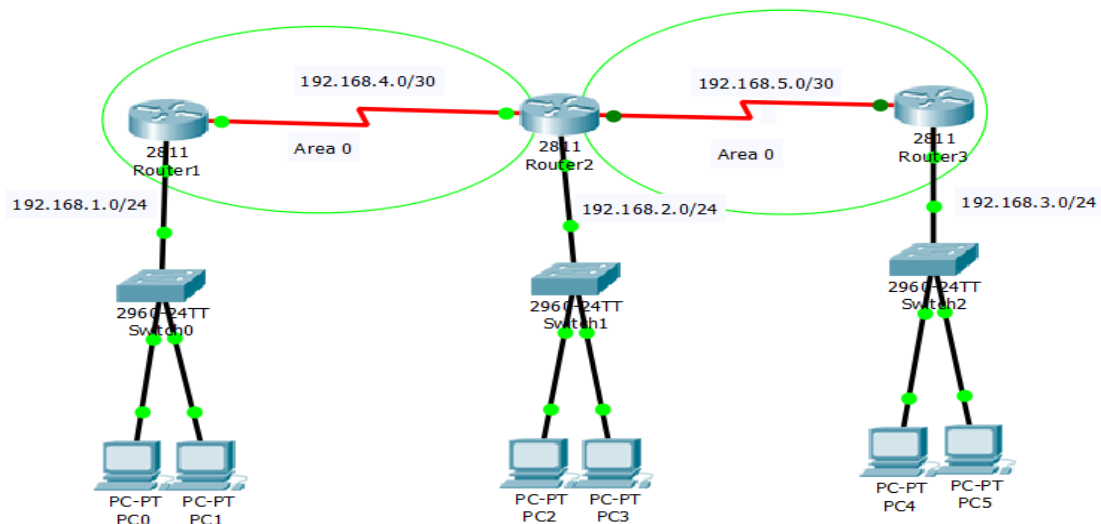
The phases of this process are-

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

5. **Discover:** Client Search for DHCP server. This discovery method is broadcast
6. **Offer:** DHCP server send offer to client. By this DHCP server shows its Presence.
7. **Request:** After getting the offer the client request for an IP address from DHCP server.
8. **Acknowledgement:** DHCP server assigned IP address to that client and send acknowledgement.

3.5 OSPF Routing Protocol:

The elaboration of OSPF is Open Shortest Path First. OSPF is a link state routing protocol based on the Open Standard. So it works on other routers including Cisco. OSPF is used as an interior gateway protocol.

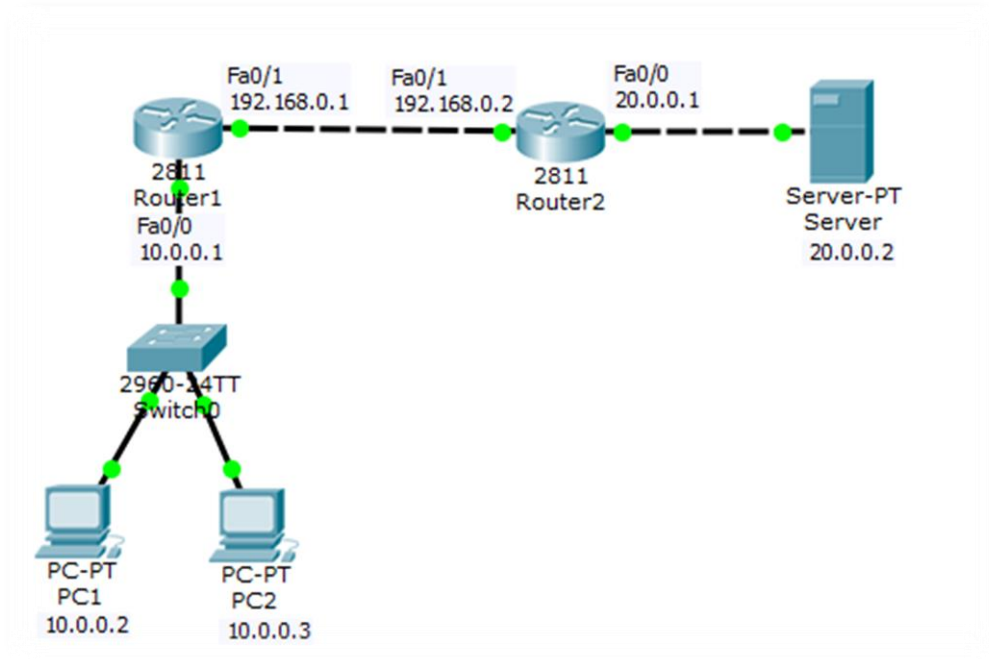


Why have we used OSPF Routing protocol in our network system?

OSPF is more useful for dynamic routing as it has more advantages than RIP. When configured OSPF will listen to neighbors and gather all link state data available to build a topology map of all available ways in their network and then save the information in their topology database, also known as its Link-State Database.

3.6 What is ACL?

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



Why we use ACL:

The main reason is ACL provides us security in networking. It provides more security on higher speed interfaces where line worth speed is necessary and firewall may be anta logistic.

3.7 SSH:

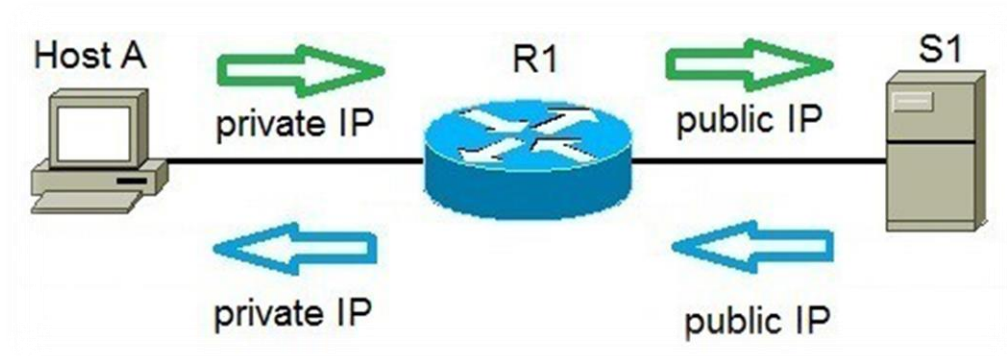
Secure shell SSH protocol is used to secure the remote login. SSH was designed to replace the unsecure remote connection Telnet. Secure shell Provides Strong authentication and encryption of communication between two computers

Why we have used SSH in our topology?

- Password is less secure than SSH.
- Non-interactive login.

3.8 NAT:

Nat means Network address translation. Using private IP address, Nat is done for using internet. To increase network security NAT is configured. Those hosts are given internet facilities, IP NAT of only for that hosts is configured

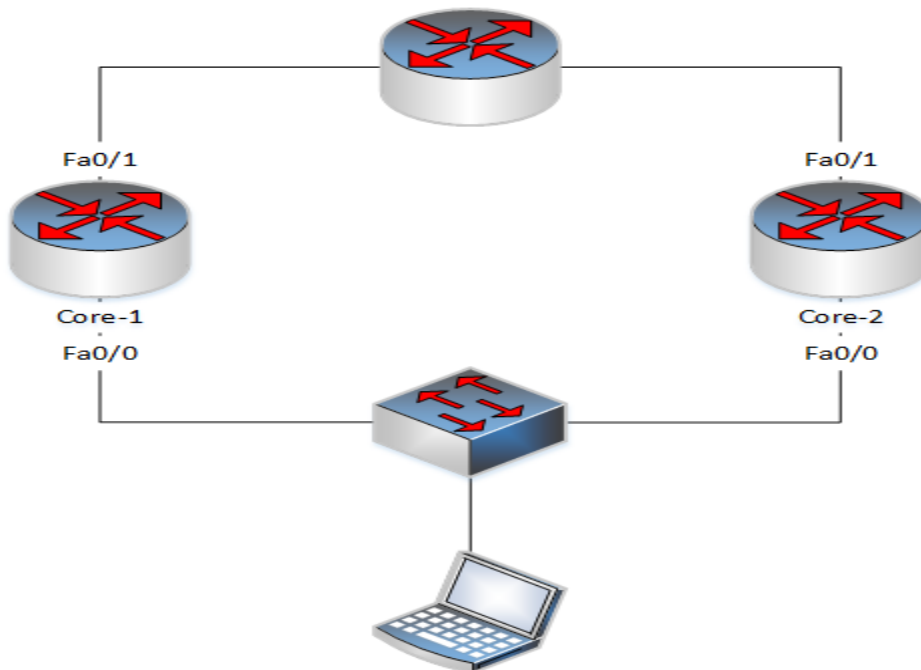


Why use to NAT in our topology:

The increase in the number of IPv4 public addresses is almost the last. So with a public IP, a private IP can be networked, netted for that.

3.9 Hot Standby Router Protocol (HSRP):

HSRP is a process by that 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.

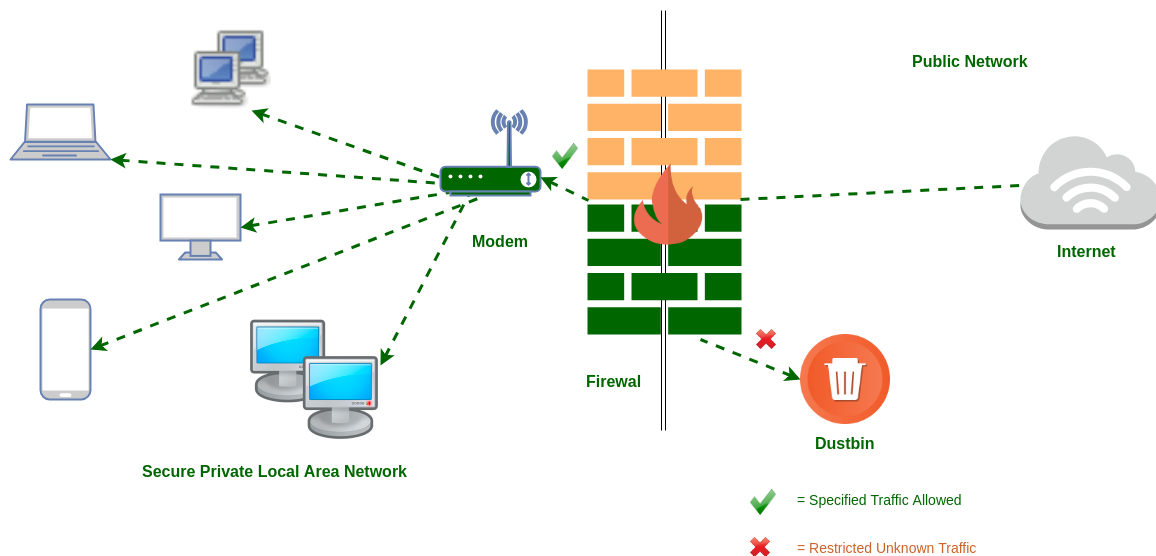


Why we have used HSRP in our topology?

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. Cisco calls its firewall an Adaptive Security Appliance (ASA). This cisco Adaptive Security Appliance is a complicated network security device that completes a stateful firewall, VPN and other abilities.



Why we have used firewall? :

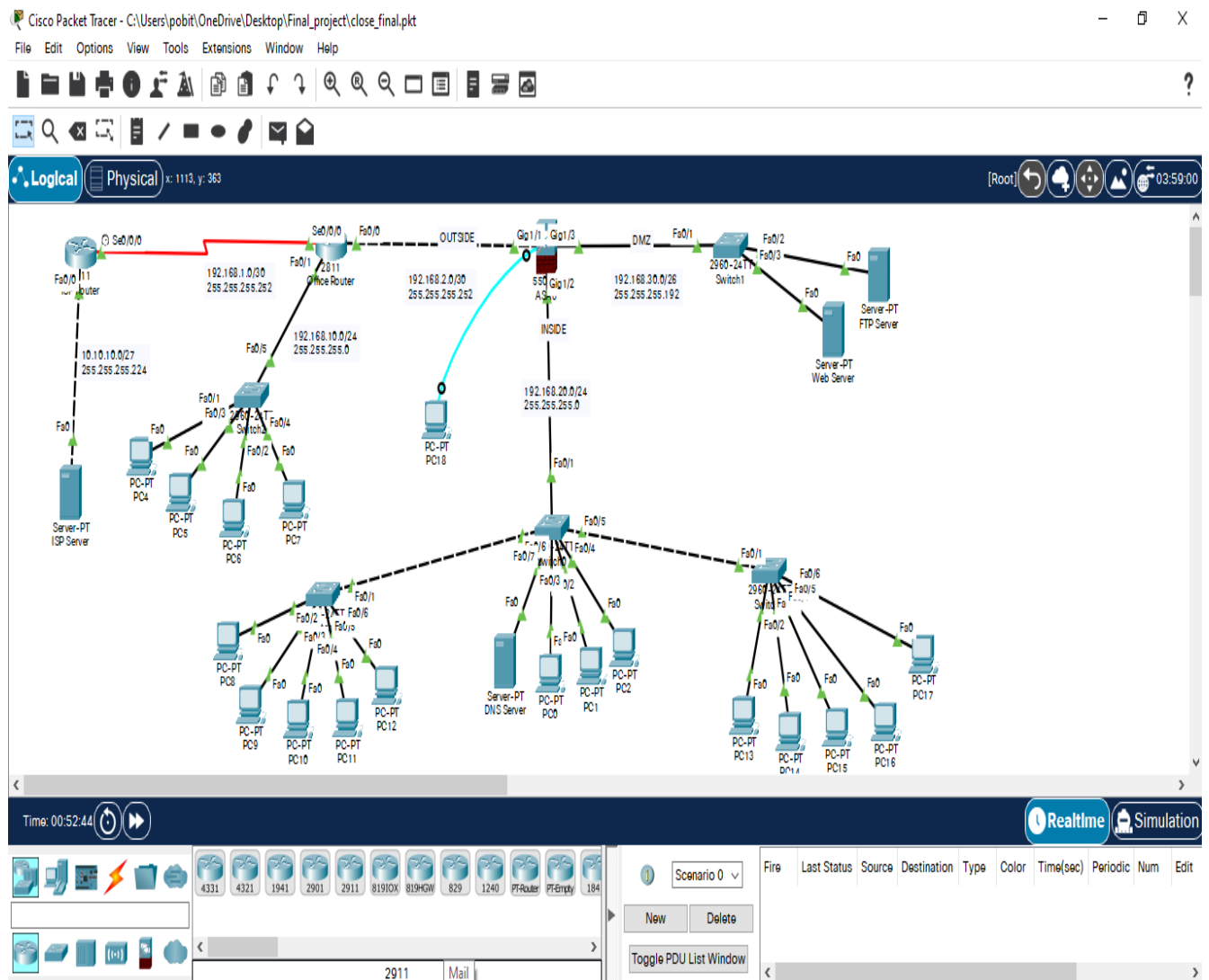
1. The reason of use firewall is given below.
2. Improving security.
3. Protecting the resources of LAN.
4. Inspection and validating incoming or outgoing traffic.
5. Giving record of its all activity.

3.11 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.



4.2 Back-end design:

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

4.3 Implementation Requirement:

Since it is a simulating software for that reason we require the imaginable software to implement our method after that we require the pre-installed network devices and there elements to implement our project.

The devices that we have used to design our network are given below:

1. Router: Router is an OSI model's layer 3 device. We have use the different models of cisco router. Like generic and 2811 series router.
2. Switch: there are mainly two types of switch. OSI Layer 2 and OSI layer 3 switch. we have use 2960 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 -

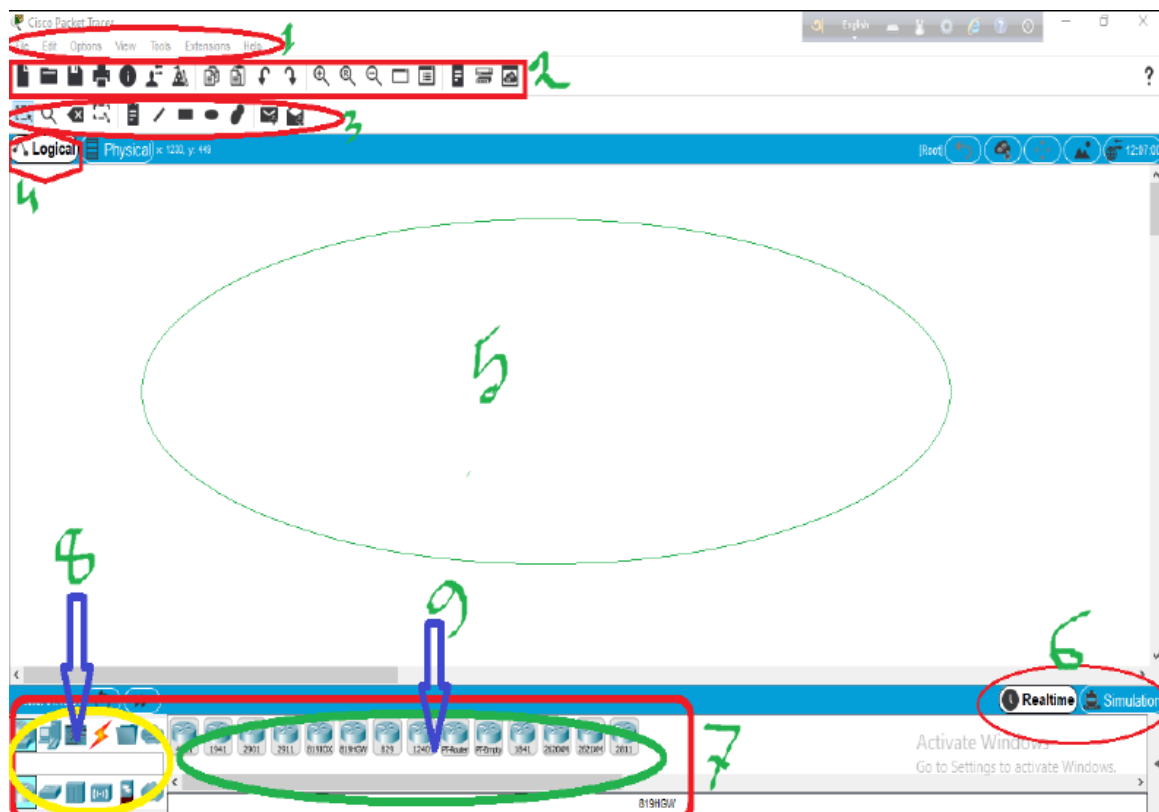
1. Fast Ethernet cable.
 2. Gigabit Ethernet cable.
 3. Serial cable.
-
6. Server: Server is a special device that supports many protocols. Like HTTP, FTP, SMTP, DCHP, TFTP

4.4 Simulator:

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.

4.5 GUI of packet tracer:

We have shown the graphical interface of cisco packet tracer in figure.



1. Menu bar
2. Main tool bar
3. Common tools bar
4. Logical/Physical workspace and navigation bar
5. Workspace
6. Real-time/Simulation bar
7. Network component box
8. Device type selection box
9. Device specification selection box

Menu bar:

This section provides the Edit, Option, File, View tools, extensions and Help menu. In this menu will find basic instructions like as Save, Open, Print and Preferences.

Main tool bar:

This section presents shortcut icons to the File and Edit menu instructions. This section also presents button for zoom, the drawing palette and the tool template manager.

Common tools bar:

This section provides access to these generally used workspace equipment choose, inspect, delete add simple PDU and add complicated PDU.

Logical/Physical workspace and navigation bar:

The physical and logical workspace with the tables on this section. In logical workspace this section grants too to navigation through levels of a Cluster, Move Object, Set Tiled Background, create a New Cluster and Viewport. In physical workspace, this section permits to navigation through physical Locations, create a New Constructing, create a New City, create a New Closet, follow grid to the Background, Move Object, Set background and go to the working Closet.

Workspace:

This region is where will create show network, simulation and view many sorts of information and records.

Real-time/Simulation bar:

This section provides buttons too to power cycle devices in summation to the play control buttons and the event list Toggle button in simulation mode. It contains a clock that shows the relative time in Real-time mode and Simulation mode.

Network component box:

This box that you choose instruments and connections to put into the workspace. It takes on the device type selection box and the device definition selection box.

Device type selection box:

The device-specification selection box will change depending on which type of device you choose.

Device specification selection box:

The box is where choose specifically which devices you want to put in network and which connections to make.

CHAPTER 5

IMPLEMENTATION AND TESTING

This chapter deals with Implementation and testing configuration screenshot.

5.1 implementation:

The Implementation of our project background code developed screenshot.

Assigning IP address into a router's port:

We have shown IP address into a Router's port in figure 5.1.1

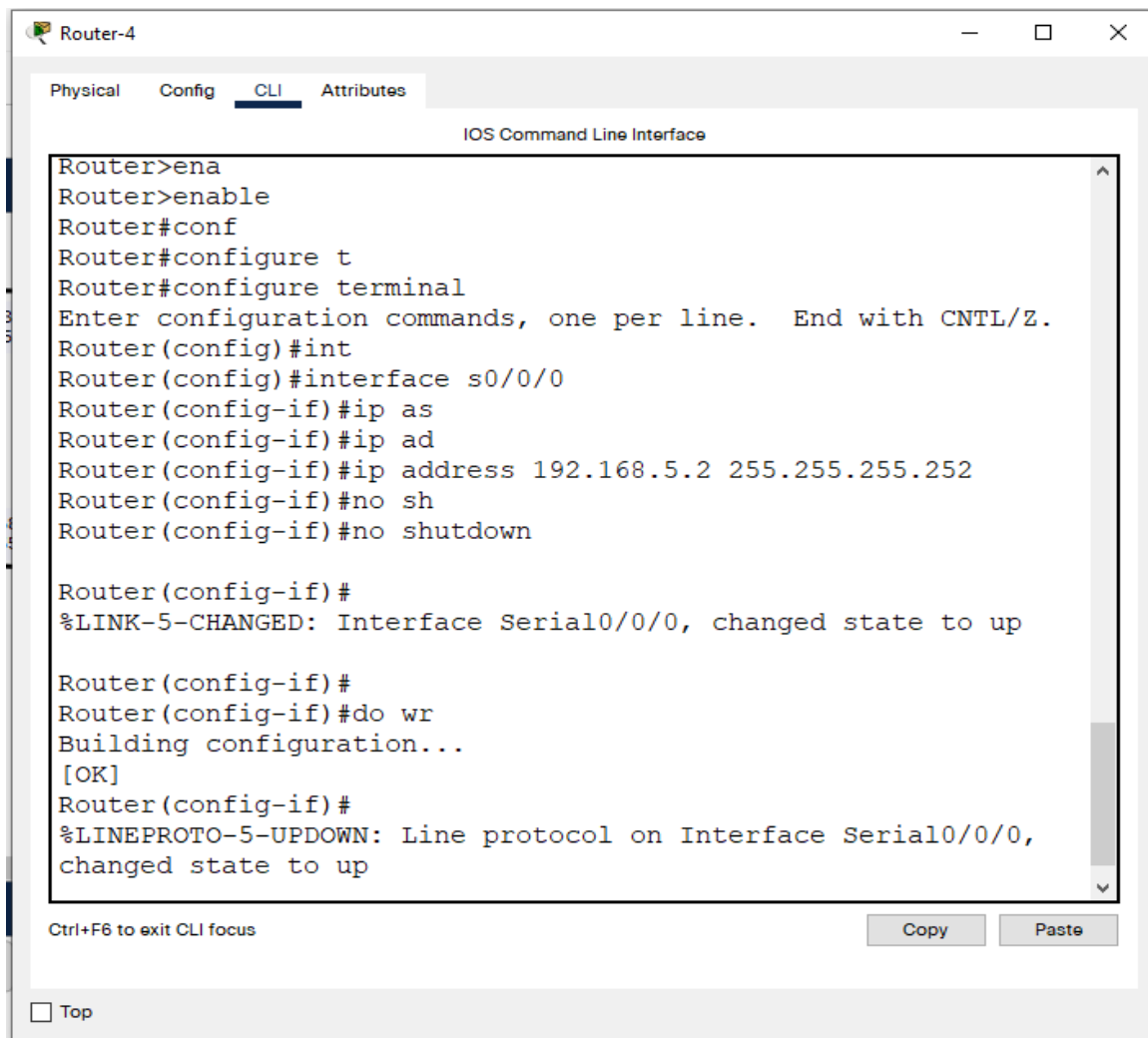


Figure-5.1.1

Password protection system of router:

We have shown Password protection system of router figure 5.1.2

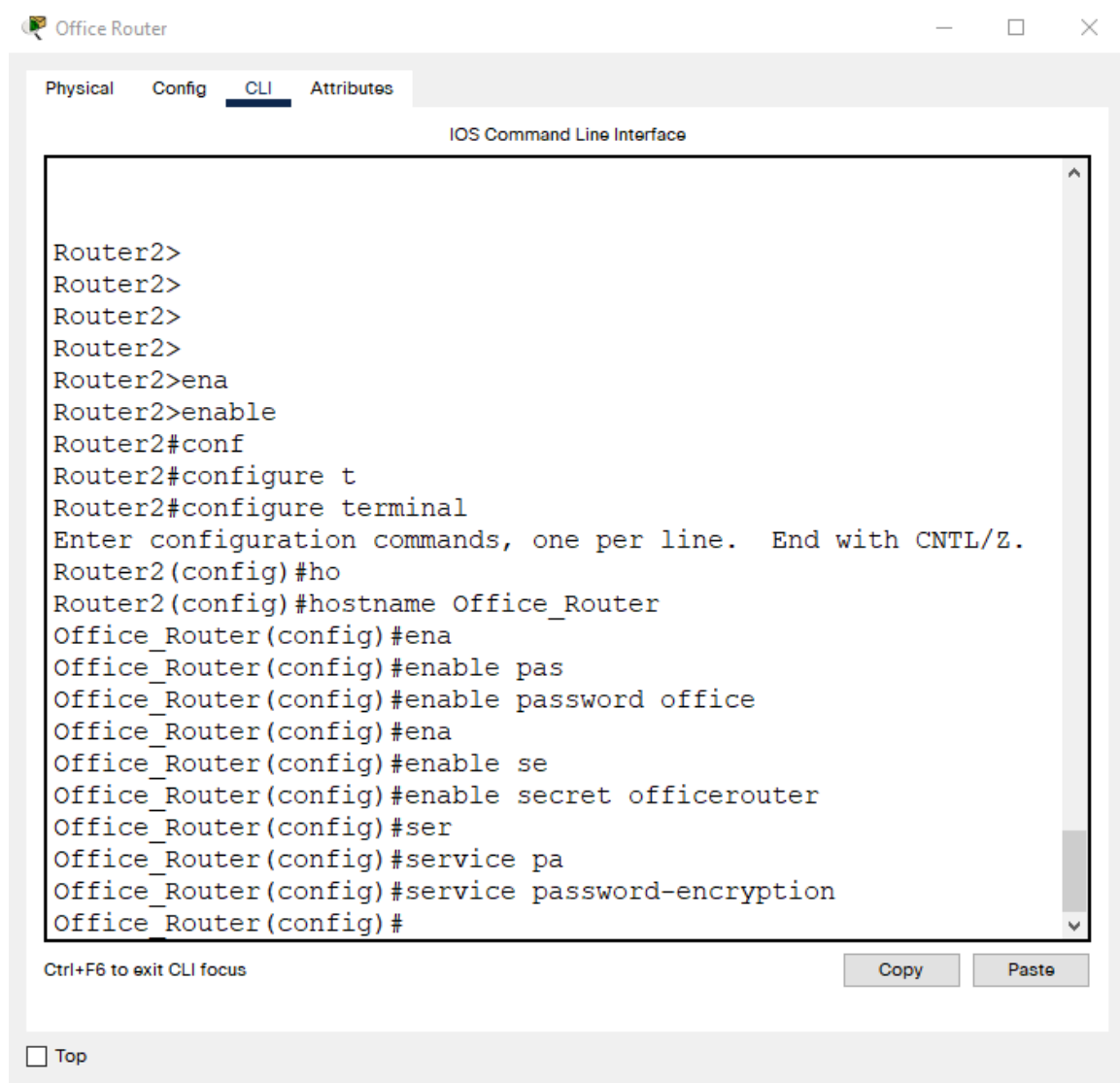


Figure-5.1.2

Assigning IP address into the pc from DHCP:

We have shown Assigning IP address into the pc from DHCP in figure 5.1.3

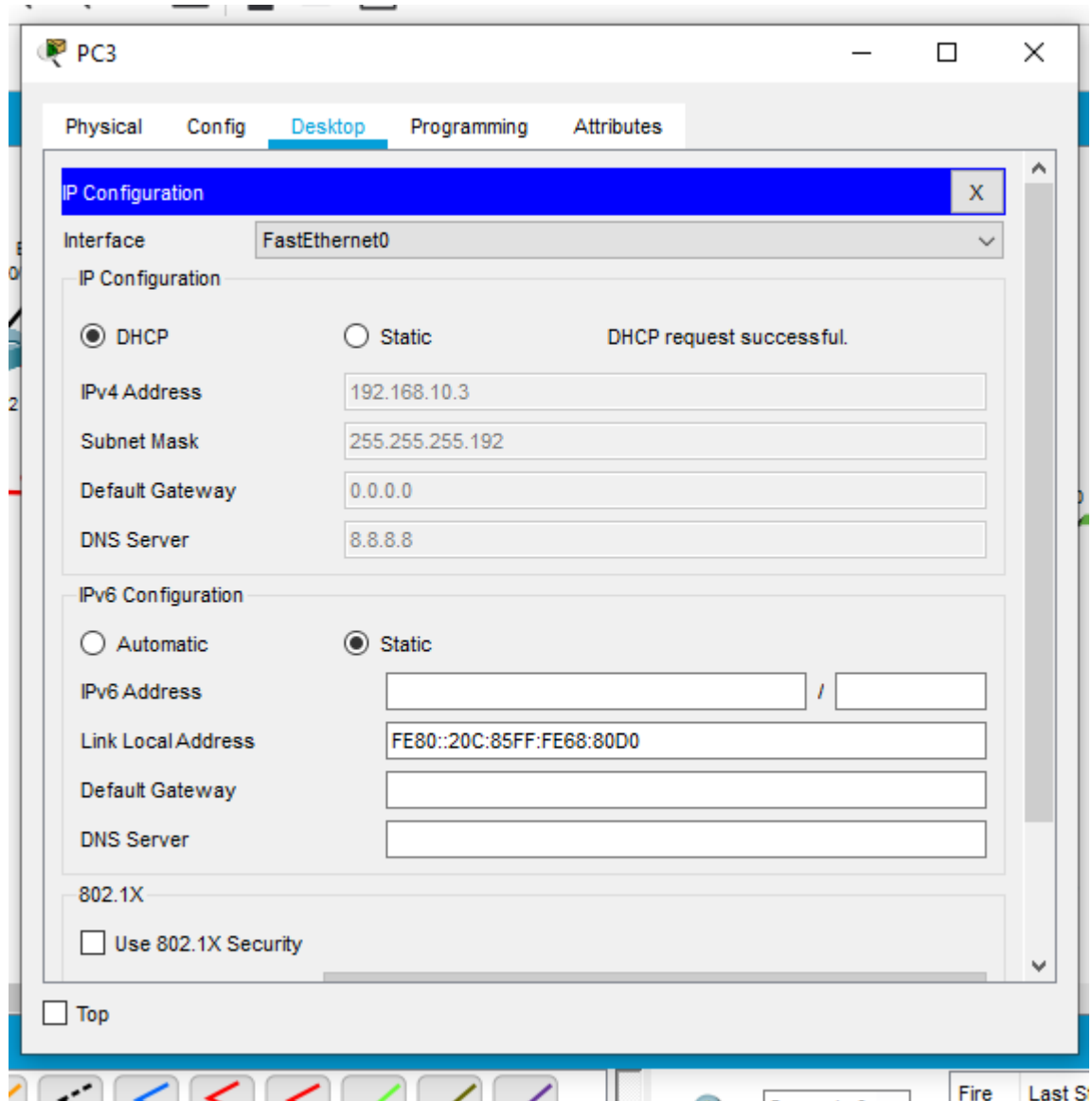
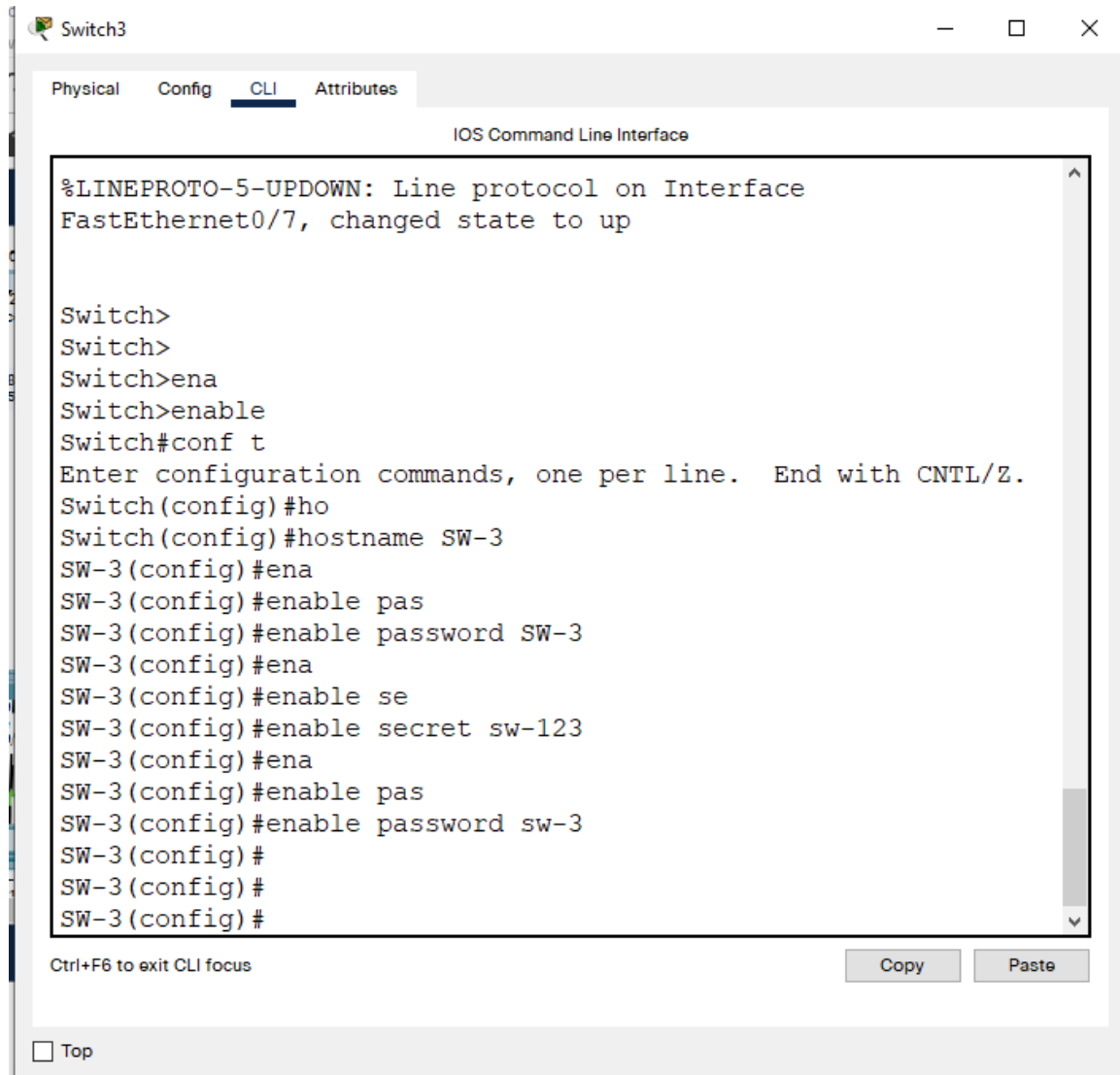


Figure-5.1.3

Password protection system of switch:

We have shown Password protection system of switch in figure 5.1.4



The screenshot shows a network switch configuration window titled "Switch3". It has tabs for "Physical", "Config", "CLI", and "Attributes", with "CLI" selected. The main area is titled "IOS Command Line Interface" and displays the following text:

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/7, changed state to up

Switch>
Switch>
Switch>ena
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ho
Switch(config)#hostname SW-3
SW-3(config)#ena
SW-3(config)#enable pas
SW-3(config)#enable password SW-3
SW-3(config)#ena
SW-3(config)#enable se
SW-3(config)#enable secret sw-123
SW-3(config)#ena
SW-3(config)#enable pas
SW-3(config)#enable password sw-3
SW-3(config)#
SW-3(config)#
SW-3(config)#
```

At the bottom of the CLI window, there is a status bar with the text "Ctrl+F6 to exit CLI focus" and two buttons: "Copy" and "Paste". Below the CLI window, there is a checkbox labeled "Top".

Figure-5.1.4

Configured VLAN:

We have shown Configured VLAN in figure 5.1.5

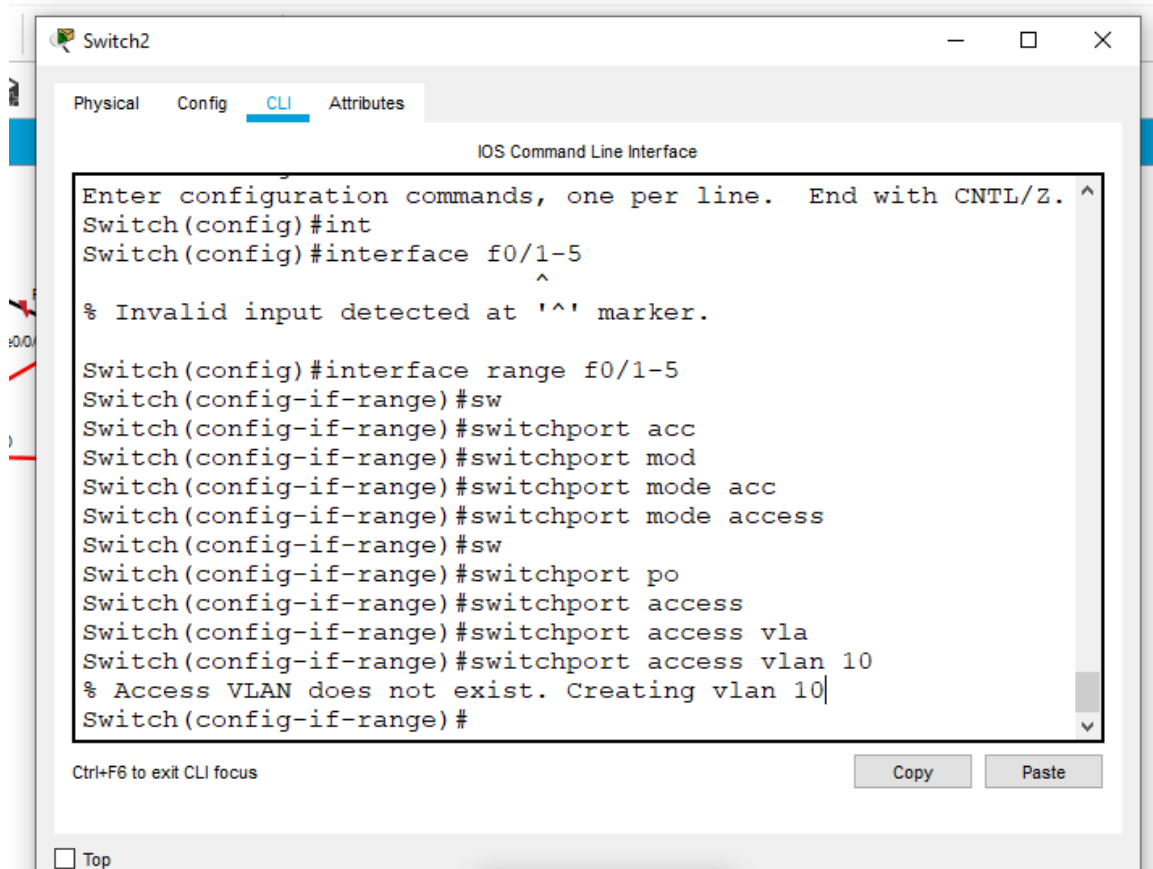


Figure-5.1.5

Configuration of Inter-VLAN:

We have shown Configured Inter-VLAN in figure 5.1.6

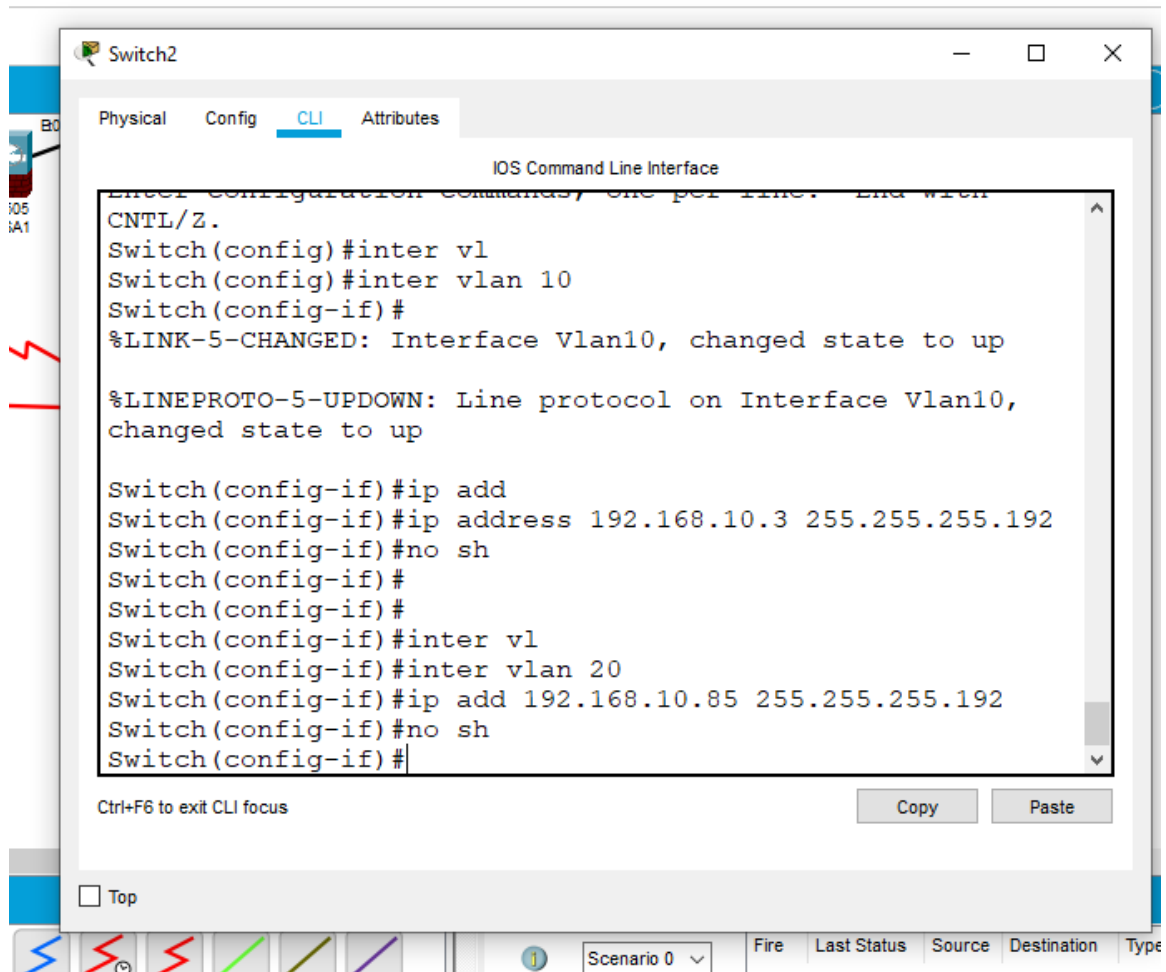


Figure-5.1.6

Configuration of Port security:

We have shown Configured Port security in figure 5.1.7

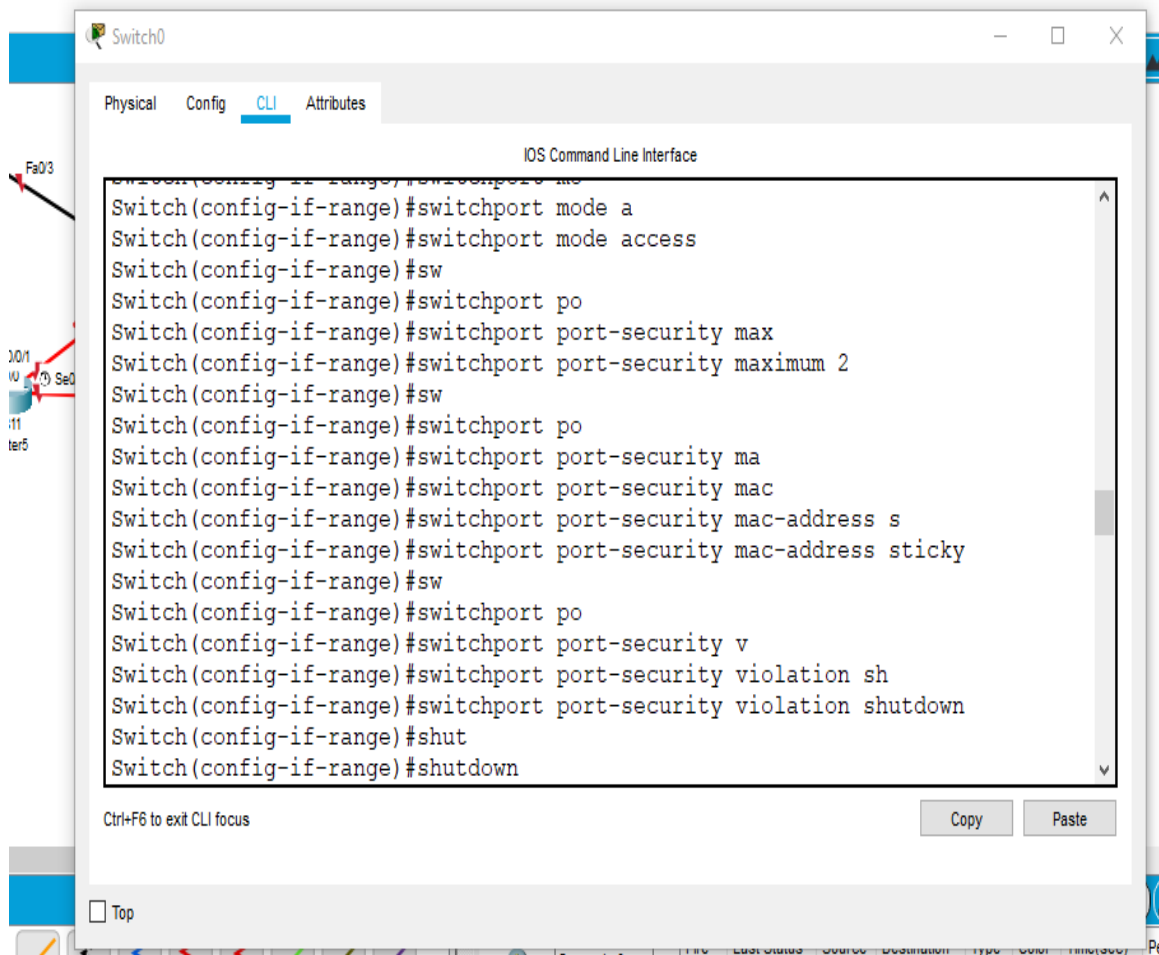
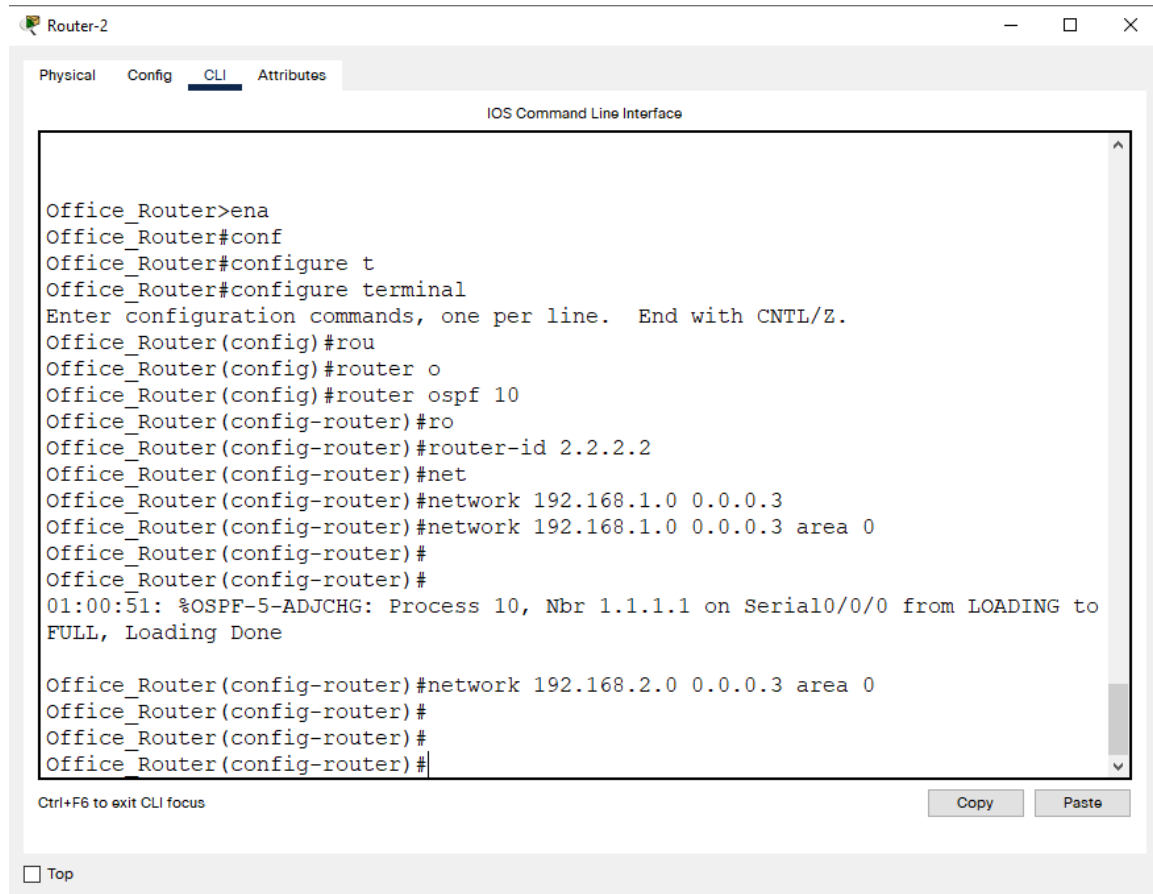


Figure-5.1.7

Configuration of OSPF Routing protocol:

We have shown Configured OSPF Routing Protocol in figure 5.1.8



The screenshot shows a Cisco IOS Command Line Interface window titled "Router-2". The window has tabs for "Physical", "Config", "CLI", and "Attributes", with "CLI" selected. The CLI shows the following commands and output:

```
Office_Router>ena
Office_Router#conf
Office_Router#configure t
Office_Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Office_Router(config)#rou
Office_Router(config)#router o
Office_Router(config)#router ospf 10
Office_Router(config-router)#ro
Office_Router(config-router)#router-id 2.2.2.2
Office_Router(config-router)#net
Office_Router(config-router)#network 192.168.1.0 0.0.0.3
Office_Router(config-router)#network 192.168.1.0 0.0.0.3 area 0
Office_Router(config-router)#
Office_Router(config-router)#
01:00:51: %OSPF-5-ADJCHG: Process 10, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to
FULL, Loading Done

Office_Router(config-router)#network 192.168.2.0 0.0.0.3 area 0
Office_Router(config-router)#
Office_Router(config-router)#
Office_Router(config-router)#
```

At the bottom of the CLI window, there is a status bar with the text "Ctrl+F6 to exit CLI focus" and two buttons: "Copy" and "Paste".

Figure-5.1.8

Configuration of Access Control List (ACL):

We have shown Configured of ACL in figure 5.1.9

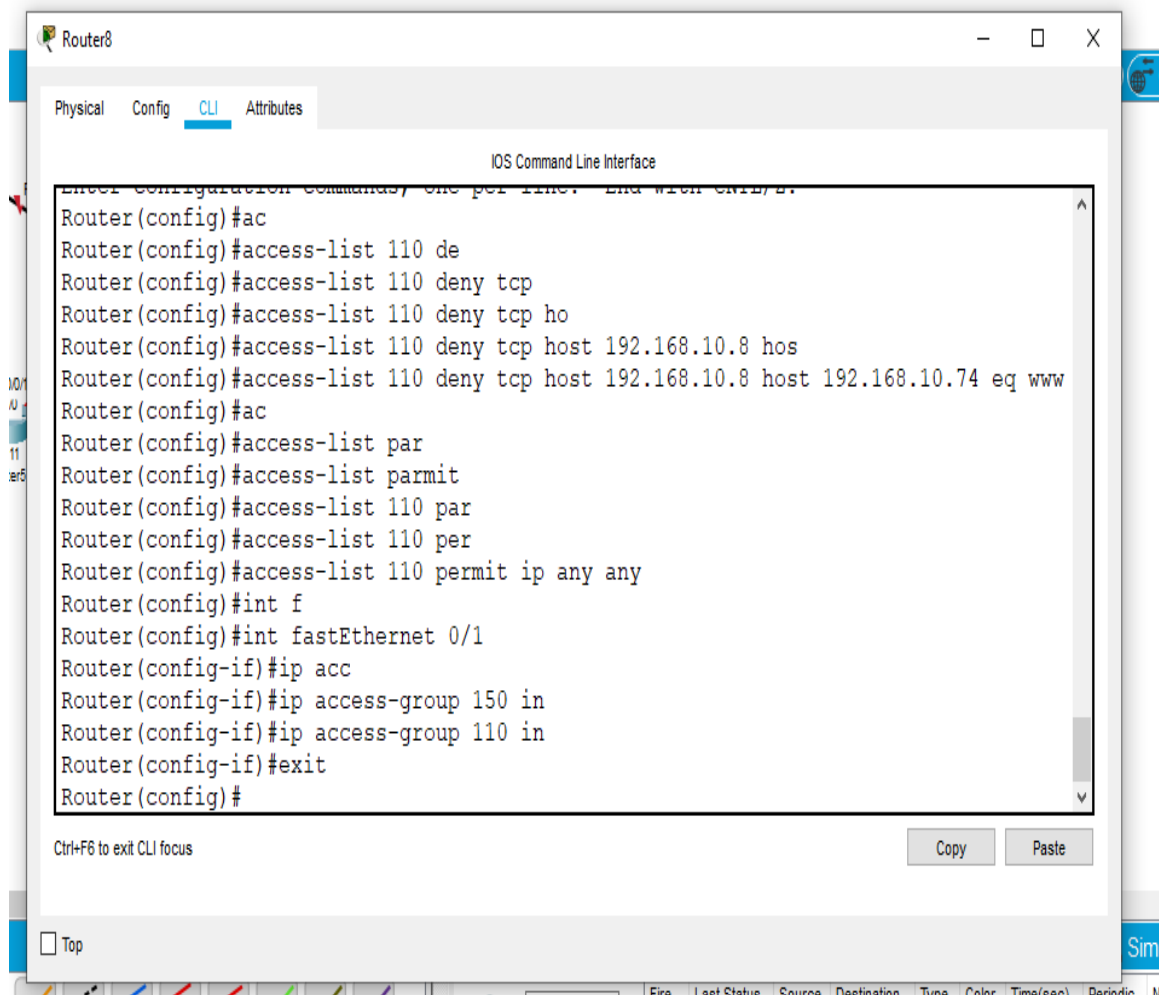
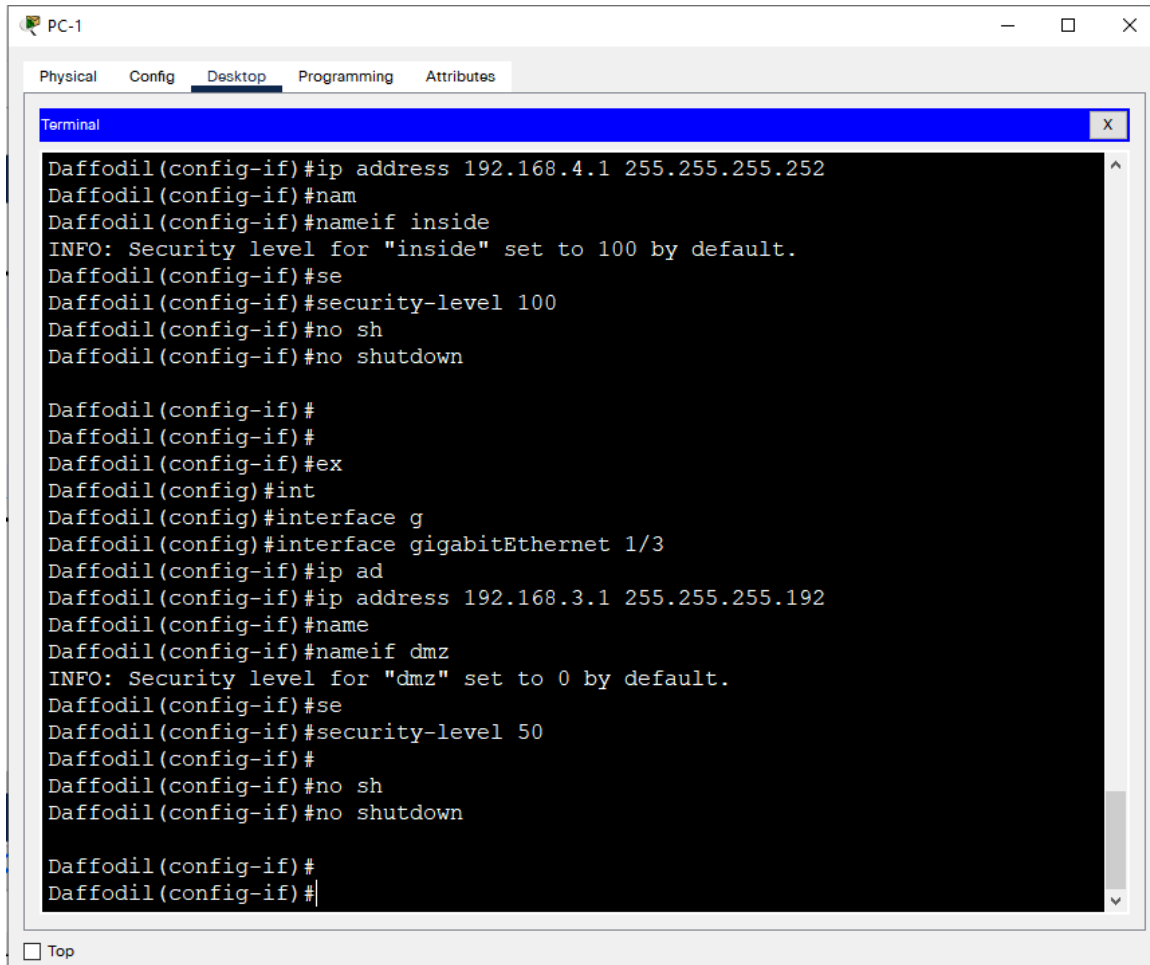


Figure-5.1.9

Configuration of ASA Firewall:

We have shown Configured ASA Firewall in figure 5.1.10



The image shows a terminal window titled "PC-1" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Terminal" tab is active, displaying a series of configuration commands for an ASA firewall. The commands are entered in a black terminal window with a blue title bar. The commands configure two interfaces: "inside" and "dmz". The "inside" interface is configured with IP address 192.168.4.1, name "inside", security level 100, and no shutdown. The "dmz" interface is configured with IP address 192.168.3.1, name "dmz", security level 50, and no shutdown. The terminal output shows the commands being entered and the resulting configuration.

```
Daffodil(config-if)#ip address 192.168.4.1 255.255.255.252
Daffodil(config-if)#nam
Daffodil(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
Daffodil(config-if)#se
Daffodil(config-if)#security-level 100
Daffodil(config-if)#no sh
Daffodil(config-if)#no shutdown

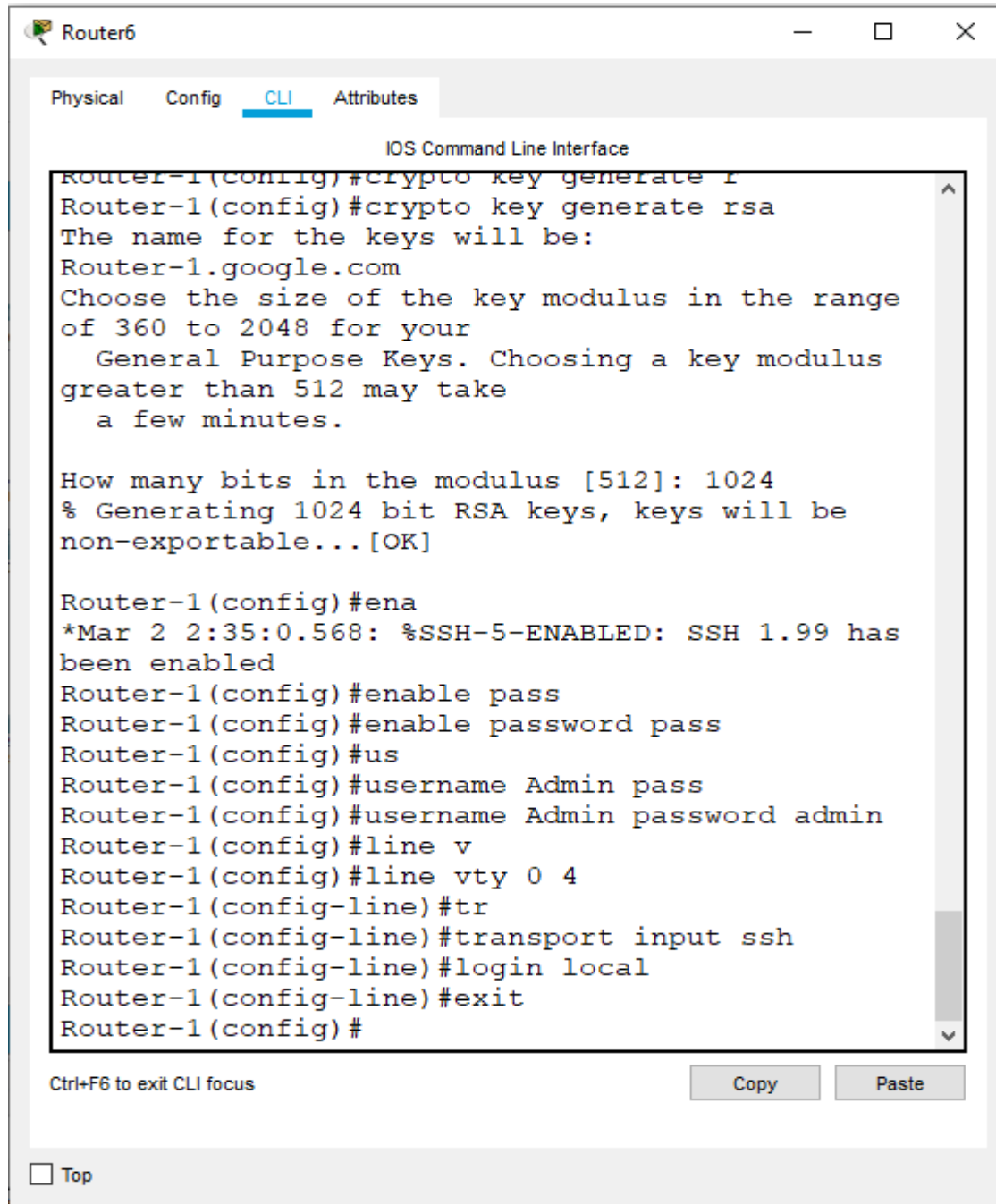
Daffodil(config-if)#
Daffodil(config-if)#
Daffodil(config-if)#ex
Daffodil(config)#int
Daffodil(config)#interface g
Daffodil(config)#interface gigabitEthernet 1/3
Daffodil(config-if)#ip ad
Daffodil(config-if)#ip address 192.168.3.1 255.255.255.192
Daffodil(config-if)#name
Daffodil(config-if)#nameif dmz
INFO: Security level for "dmz" set to 0 by default.
Daffodil(config-if)#se
Daffodil(config-if)#security-level 50
Daffodil(config-if)#
Daffodil(config-if)#no sh
Daffodil(config-if)#no shutdown

Daffodil(config-if)#
Daffodil(config-if)#
```

Figure-5.1.10

Configuration of SSH:

We have shown Configured SSH in figure 5.1.11



The screenshot shows a window titled "Router6" 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 responses:

```
Router-1(config)#crypto key generate rsa
Router-1(config)#crypto key generate rsa
The name for the keys will be:
Router-1.google.com
Choose the size of the key modulus in the range
of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus
greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be
non-exportable...[OK]

Router-1(config)#ena
*Mar 2 2:35:0.568: %SSH-5-ENABLED: SSH 1.99 has
been enabled
Router-1(config)#enable pass
Router-1(config)#enable password pass
Router-1(config)#us
Router-1(config)#username Admin pass
Router-1(config)#username Admin password admin
Router-1(config)#line v
Router-1(config)#line vty 0 4
Router-1(config-line)#tr
Router-1(config-line)#transport input ssh
Router-1(config-line)#login local
Router-1(config-line)#exit
Router-1(config)#
```

At the bottom of the CLI window, there is a status bar with the text "Ctrl+F6 to exit CLI focus" and two buttons: "Copy" and "Paste". Below the CLI window, there is a checkbox labeled "Top".

Figure-5.1.11

5.2 Testing Implementation:

The testing implementation of our project screenshot.

Ping the Packet Transfer:

We have shown packet transfer in figure 5.2.1

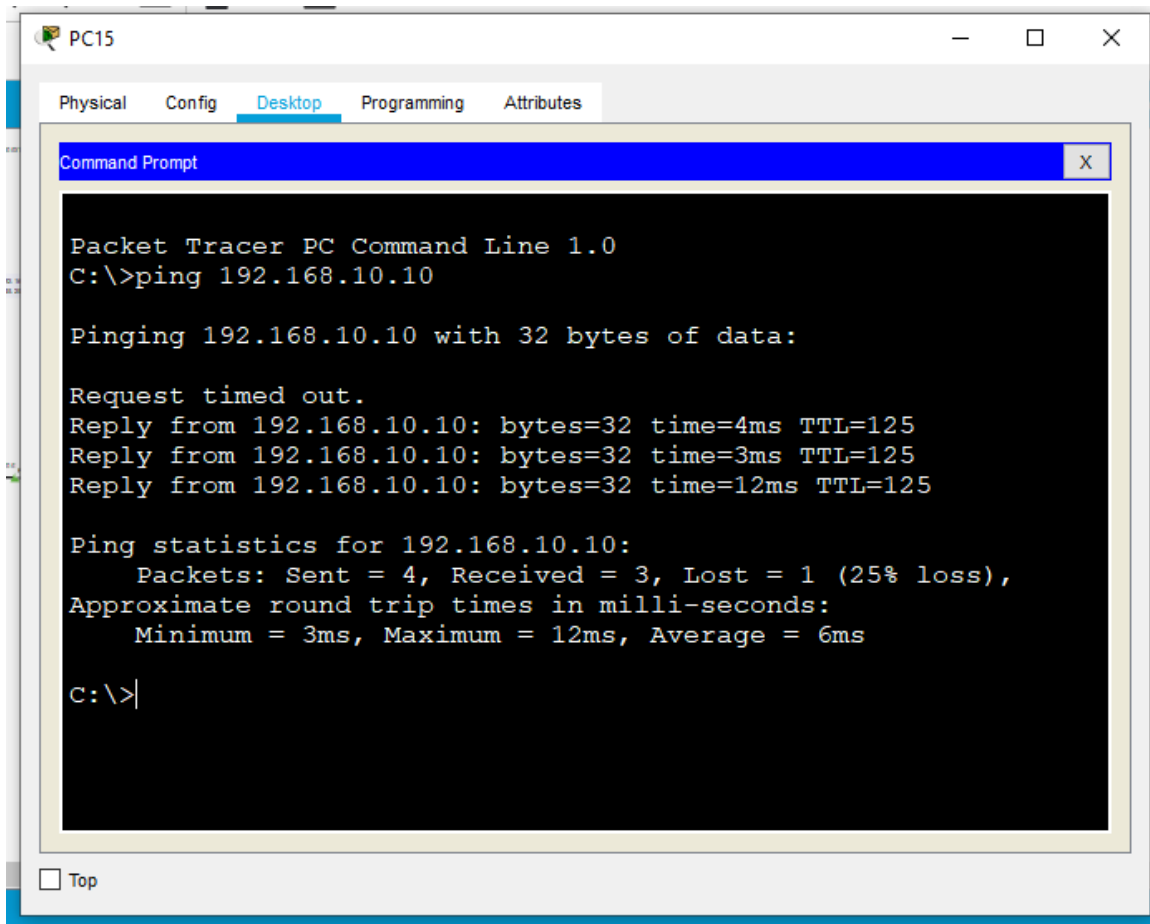


Figure-5.2.1

Checking the Routing:

We have shown checking the Router in figure 5.2.2

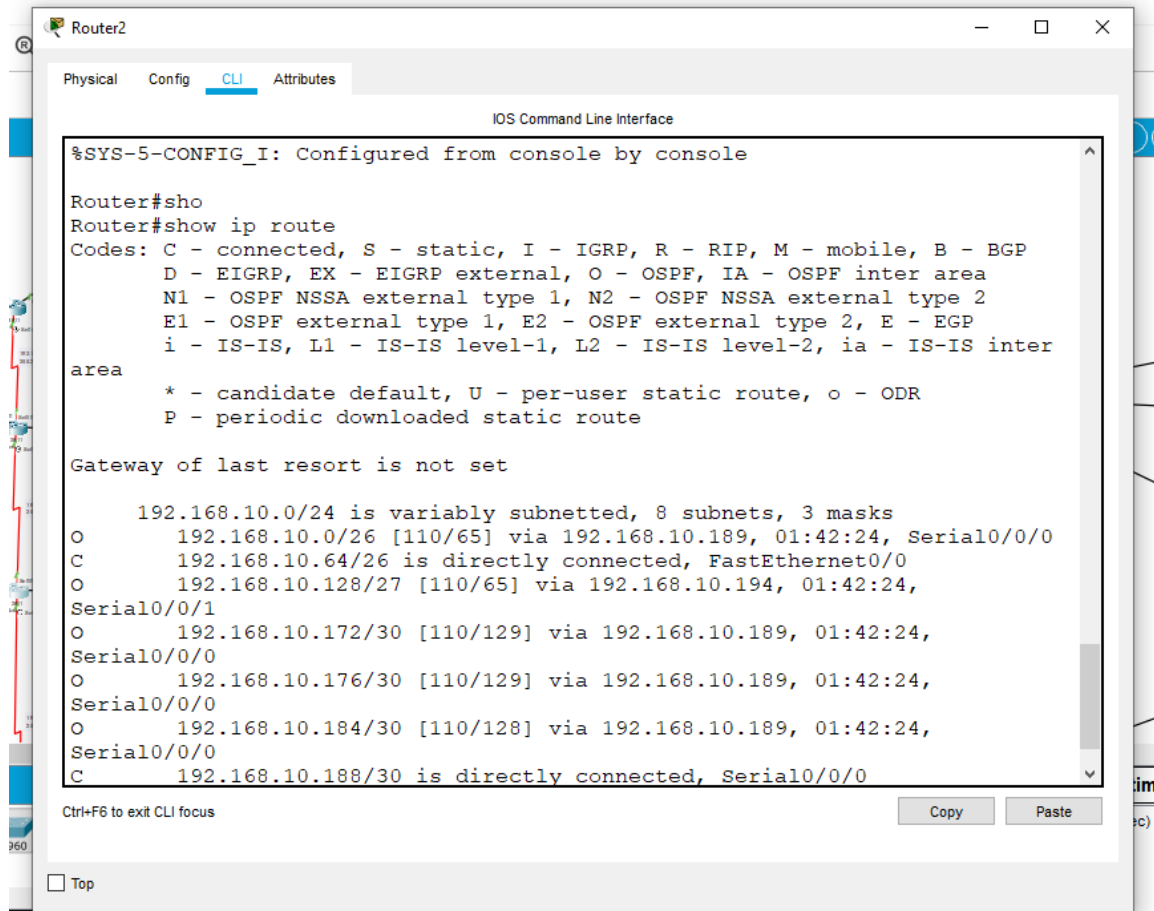


Figure 5.2.2

CHAPTER 7

CONCLUSION AND FUTURE SCOPE

7.1 Discussion and Conclusion:

Making security and maintaining it's far a very difficult challenge. Our task can make sure the structural and topological security. We've got tried to provide security with the available devices with their constructed in configuration, without the usage of any sort of extra software program. And the security methods that we've used Like ACL, VPN, port security, Secured Shell (SSH), Console passwords are the modern technology to provide community protection. However our project has a few limitations.

7.2 Scope for Further Developments:

We will also update our project if any advanced technology appears in the future to secure the network structure. And we will try to implement this topology in any new corporate office.

REFERENCES:

- [1] B. K. R. B. A. M. P. N.Hari Prasad, "Intervlan Routing and Various Configurations," IJIRST –International Journal for Innovative Research in Science & Technology, vol. 2, no. 11, pp. 749-758, April 2016.
- [2] G. Thrivikram, "STUDY AND SIMULATION OF OSPF," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), vol. 7, no. 2, pp. 45-47, April 2016.
- [3] E. A. A. Shipra Suman, "IP Traffic Management With Access Control List Using Cisco Packet Tracer," International Journal of Science, Engineering and Technology Research (IJSETR), vol. 5, no. 5, pp. 1556-1561, May 2016.
- [4] G. 1Anchit Bansal, "Simulation and Analysis of Network Address Translation (NAT)," Anchit Bansal. Int. Journal of Engineering Research and Application, vol. 7, no. 7, pp. 50-56, July 2017.
- [5] R. R. V.Selvi1, "The Design and Implementation of On-Line Examination Using Firewall security," OSR Journal of Computer Engineering (IOSR-JCE), vol. 16, no. 6, pp. 20-24, Nov – Dec. 2014.
- [6] Schudel, Gregg, and David Smith. Router security strategies: Securing IP network traffic planes. Pearson Education, December 2007.
- [7] D. a. M. A. Dr.G.Padmavathi1, "ANODR-ECC Key Management protocol with," International Journal of Distributed and Parallel Systems (IJDPS), vol. 3, no. 1, pp. 331-339, January 2012.
- [8] D. T. R. Draves, "default route," Default Router Preferences and More-Specific Routes, vol. 5, no. 6, pp. 03-06, November 2005.
- [9] V.Selvi1, "The Design and Implementation of On-Line Examination Using," IOSR Journal of Computer Engineering (IOSR-JCE), vol. 16, no. 6, pp. 20-24, Sun, 13 Jan

2019.

- [10] A. Chopra, "Security Issues of Firewall," International Journal of P2P Network Trends and Technology (IJPTT), vol. 22, no. 1, pp. 4-8, January 2016.
- [11] B. J. M. Thaier Hayajneh, "Performance and Information Security Evaluation with," International Journal of Security and Its Applications, vol. 7, no. 6, pp. 355-372 , 2013.
- [12] X. Rong-Rong and Y. Xiao-Chun, "Improving network security using genetic algorithm approach," Published by Jossey-Bass, A Wiley Company. Reprinted by permission of John Wiley &, vol. 33, no. 5-6, pp. 438-451, September–November 2007.
- [13] P. Airi, "Cisco Packet Tracer as a teaching and learning tool for computer networks in DWU," Airi & Anderson, Cisco Packet Tracer as a teaching and learning tool for computer, pp. 88-108, May 2017.
- [14] Gaudet N, Sahu A, Goulart AE, Rogers E, Davis K. Firewall configuration and path analysis for smartgrid networks. In 2020 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR) 14 pp. 16) May 2020
- [15] A. A. N. a. A. A. K. H. Bourdoucen, "Impact of Implementing VPN to Secure," World Academy of Science, Engineering and Technology, pp. 625-630, 2009.
- [16] M. E. I. N. A. S. L. Glend Sondakh, "Perancangan Filtering Firewall Menggunakan Iptables Di Jaringan Pusat Teknologi Informasi Unsrat," Jurnal Teknik Elektro dan Komputer, vol. 3, no. 4, 2014.
- [17] D. P. Satasiya, "Enhanced Sdn Security Using Firewall," Gujarat Technological University, Ahmedabad, May, 2016.

IMPROVING COMPUTER NETWORK SECURITY

ORIGINALITY REPORT

24%	23%	0%	20%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Daffodil International University Student Paper	5%
2	www.coursehero.com Internet Source	4%
3	tintabening.blogspot.com Internet Source	4%
4	www.pctresearchgroup.com Internet Source	2%
5	college.ac Internet Source	2%
6	dspace.daffodilvarsity.edu.bd:8080 Internet Source	2%
7	Submitted to ACIT Student Paper	1%
8	www.guru99.com Internet Source	1%
9	www.geeksforgeeks.org Internet Source	1%