Bus Depot Station Network Design

Virtual Cybersecurity Internship 2021 Report

Submitted

To

Centre of Excellence

Cybersecurity & Networking

Duration 6 Weeks Virtual Internship

By

ASTHA GUPTA

1803213038

ABES Engineering College

Abdul Kalam Technical University

Under the guidance of
KRISHNA VIR SINGH

DECLARATION

I hereby declare that the Project Report entitled **"Bus Depot Station Network Design"** under the course name **"AICTE Virtual Cybersecurity Internship"** in Department of "Information Technology" of "ABES ENGINEERING COLLEGE" is an authentic record of my own work carried out under the supervision of **MR. KRISHNA VIR SINGH**

Dated:

Signature of student:

Name: ASTHA GUPTA

Roll No: 1803213038

Department: IT

This to certify that the above statements made by the candidate are true and correct to the best of my knowledge.

Signature of Supervisor

ACKNOWLEDGEMENT

It gives me a great sense of pleasure to present the report of the Project Based Internship 2021 undertaken during AICTE Virtual Cybersecurity Internship. I owe special debt of gratitude to Krishna Vir Singh, Centre of Excellence: Cybersecurity & Networking for his constant support and guidance throughout the course of our work. His constant motivation has been a constant source of inspiration for us. It is only his cognizant efforts that our endeavors have seen light of the day.

I also take the opportunity to acknowledge the contribution of team members of Centre of Excellence: Cybersecurity & Networking for their full support and assistance during the development of the project.

I also do not like to miss the opportunity to acknowledge the motivation of the Information Technology Department and ABES Engineering College to provide us the opportunity to undergo AICTE Virtual Cybersecurity Internship at the Centre of Excellence: Cybersecurity & Networking.

Signature: *Astha Gupta*

Name : ASTHA GUPTA

Roll No.: 1803213038

Date : June 28,2021

ABSTRACT

Cyber Security Plays an important role in the field of information technology. Securing the information has become one of the biggest challenges in the present day. Whenever we think about cyber security the first thing that comes to our mind is “cyber crimes” which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cybercrimes. Besides various measures cyber security is still a very big concern to many.

Network Security protects your network and data from breaches, intrusions and other threats. This is a vast and overarching term that describes hardware and software solutions as well as processes or rules and configurations relating to network use, accessibility, and overall threat protection.

A good network security system helps businesses reduce the risk of falling victim to data theft and sabotage. Network security helps protect your workstations from harmful spyware. It also ensures that shared data is kept secure.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

COURSE DESCRIPTION

Begin preparing for a networking career with this introduction to how networks operate. This first course in the 3-course CCNA series introduces architectures, models, protocols, and networking elements – functions needed to support the operations and priorities of Fortune 500 companies to small innovative retailers. You'll even get the chance to build simple local area networks (LANs). Developing a working knowledge of IP addressing schemes, foundational network security, you'll be able to perform basic configurations for routers and switches. No prerequisites required. After completing all three CCNA courses, you are ready to take the CCNA Certification.

You'll Learn These Core Skills:

Build simple LANs, perform basic configurations for routers and switches, and implement IPv4 and IPv6 addressing schemes.

Configure routers, switches, and end devices to provide access to local and remote network resources and to enable end-to-end connectivity between remote devices . Develop critical thinking and problem-solving skills using real equipment and Cisco Packet Tracer . Configure and troubleshoot connectivity a small network using security best practices. Designed for Distance Learning

A distance learning option is available for this course. Lab activities can be completed with Packet Tracer if lab equipment is not available.

CHAPTER 2

INTRODUCTION

2.1 Aim of the Project: To design a secure network for Bus Depot Station.

2.2 Objective of the Project:

- Simulate the typical network architecture for "Bus Depot Network" on packet tracer tool, wherein End User can book the ticket by accessing Bus Depot website/Application via their own devices (Desktop/Laptop/Mobile).
- Demonstrate the concept of IP addressing, VLAN segmentation, CIDR, WLAN using various network devices like Core Switch (L3), Access Switches, routers, WLAN, Access points, servers and endpoints (Desktops/Laptops/Mobile devices)

2.3 Scope of the Project:

Creating the following:

- Separate segments for WEB, APP and DB
- Separate User segments for various IT and NON-IT department like Billing, Accounts, Admin etc.
- ISP connectivity to Web Server for End user to connect to website/application.

- WLAN and Wireless access points.

2.4 Future Scope of the Project:

Use of Network Firewall to restrict and filter both inbound and outbound traffic from the network. Also to restrict the access and traffic flow in the internal network. Use NAT rules to translate the private (not globally unique) addresses in the internal network into legal addresses (Public IP), before packets are forwarded to another network.

CHAPTER 3

DESCRIPTION

A bus garage, also known as a bus depot, bus base or bus barn, is a facility where buses are stored and maintained. In many conurbations, bus garages are on the site of former car barns or tram sheds, where trams (streetcars) were stored, and the operation transferred to buses. In other areas, garages were built to replace horsebus yards or on virgin sites when populations were not as high as now.

•We need to simulate the typical network architecture for "Bus Depot Network" on packet tracer tool, wherein End User can book the ticket by accessing Bus Depot website/Application via their own devices (Desktop/Laptop/Mobile).

• Demonstrate the concept of IP addressing, VLAN segmentation, CIDR, WLAN using various network devices like Core Switch (L3), Access Switches, routers, WLAN, Access points, servers and endpoints (Desktops/Laptops/Mobile devices).

CHAPTER 4

TOOL DESCRIPTION

Tool Name: Packet Tracer

4.1 Introduction to Packet Tracer: Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts.

4.2 Different tools in Packet Tracer:

4.2.1 Network Devices

a. Switch:

A network switch is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. It is a multiport network bridge that uses MAC addresses to forward data at the data link layer (layer 2) of the OSI model.

b. Multi-Layer Switch:

Multilayer switches support Switch Virtual Interfaces (SVIs), logical interfaces that can perform routing. They behave like a physical interface of a router: they have an IP address, and they insert a connected route into the routing table. However, they are completely virtual.

c. Router:

A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork (e.g., the Internet) until it reaches its destination node.

d. Wireless Access Point:

wireless access point (WAP), or more generally just access point (AP), is a networking hardware device that allows other Wi-Fi devices to connect to a wired network. As a standalone device, the AP may have a wired connection to a router, but, in a wireless router, it can also be an integral component of the router itself. An AP is differentiated from a hotspot which is a physical location where Wi-Fi access is available.

4.2.2 Cables

a. Straight-Through Cable:

Straight-through cable is a type of twisted pair copper wire cable for local area network (LAN) use for which the RJ-45 connectors at each end have the same pinout (i.e., arrangement of conductors). Straight-through cable is also commonly referred to as patch cable.

b. Crossover Cable:

A crossover cable is a type of twisted pair copper wire cable for LANs (local area network) in which the wires on the cable are crossed over so that the receive

signal pins on the RJ-45 connector on one end are connected to the transmit signal pins on the RJ-45 connector on the other end.

4.2.3 End Devices

a. PC (Personal Computer):

A personal computer (PC) is a multi-purpose computer whose size, capabilities, and price make it feasible for individual use. Personal computers are intended to be operated directly by an end user, rather than by a computer expert or technician. Unlike large, costly minicomputers and mainframes, time-sharing by many people at the same time is not used with personal computers.

b. Laptop:

A laptop, laptop computer, or notebook computer is a small, portable personal computer (PC) with a screen and alphanumeric keyboard. These typically have a "clamshell" form factor, typically having the screen mounted on the inside of the upper lid and the keyboard on the inside of the lower lid, although 2-in-1 PCs with a detachable keyboard are often marketed as laptops or as having a "laptop mode." Laptops are folded shut for transportation, and thus are suitable for mobile use. Its name comes from lap, as it was deemed practical to be placed on a person's lap when being used. Today, laptops are the used in a variety of settings, such as at work, in education, for playing games, web browsing, for personal multimedia, and general home computer use.

c. Mobile Phone:

A mobile phone, cellular phone, cell phone, cellphone, handphone, or hand phone, sometimes shortened to simply mobile, cell or just phone, is a portable telephone that can make and receive calls over a radio frequency link while the user is moving within a telephone service area. The radio frequency link establishes a connection to the switching systems of a mobile phone operator, which provides access to the public switched telephone network (PSTN).

d. Server:

A server is a piece of computer hardware or software (computer program) that provides functionality for other programs or devices, called "clients". This architecture is called the client–server model. Servers can provide various functionalities, often called "services", such as sharing data or resources among multiple clients, or performing computation for a client. A single server can serve multiple clients, and a single client can use multiple servers. A client process may run on the same device or may connect over a network to a server on a different device. Typical servers are database servers, file servers, mail servers, print servers, web servers, game servers, and application servers.

CHAPTER 5

IMPLEMENTATION AND RESULTS

5.1 Implementation:

By using Packet Tracer, the following network is created for Bus Depot System.

5.1.1 Segmentation:

There are 10 segments in the network topology, which are as follows:

Segment-1: WLAN

It is created in VLAN 1.

IP Address ranges from 192.168.1.1 to 192.168.1.255

Segment-2: Admin Management

It is created in VLAN 2.

IP Address ranges from 192.168.2.1 to 192.168.2.255

Segment-3: Account Department

It is created in VLAN 3.

IP Address ranges from 192.168.3.1 to 192.168.3.255

Segment-4: Reservation Department

It is created in VLAN 4.

IP Address ranges from 192.168.4.1 to 192.168.4.255

Segment-5: Billing Department

It is created in VLAN 5.

IP Address ranges from 192.168.5.1 to 192.168.5.255

Segment-6: Database Server

It is created in VLAN 6.

IP Address ranges from 192.168.6.1 to 192.168.6.255

Segment-7: Web Server

It is created in VLAN 7.

IP Address ranges from 192.168.7.1 to 192.168.7.255

Segment-8: Support Server

It is created in VLAN 8.

IP Address ranges from 192.168.8.1 to 192.168.8.255

Segment-9: App Server

It is created in VLAN 9.

IP Address ranges from 192.168.9.1 to 192.168.9.255

Segment-10: L3 Switch connection to Router

IP Address ranges from 192.168.10.1 to 192.168.10.255

Segment-11: Outside Network

IP Address ranges from 192.168.11.1 to 192.168.11.255

5.1.2 Commands Used:

a. Basic configuration:

1. enable
2. configure terminal
3. hostname
4. enable secret password
5. service password-encryption
6. banner motd

b. VLans Command:

1. int fa0/0
2. switchport mode access
3. switch access vlan
4. ip routing
5. ip add 192.168.1.0 255.255.255.0
6. no shutdown

c. Checking Connectivity

ping ip address

5.2 Screenshots of the Result:

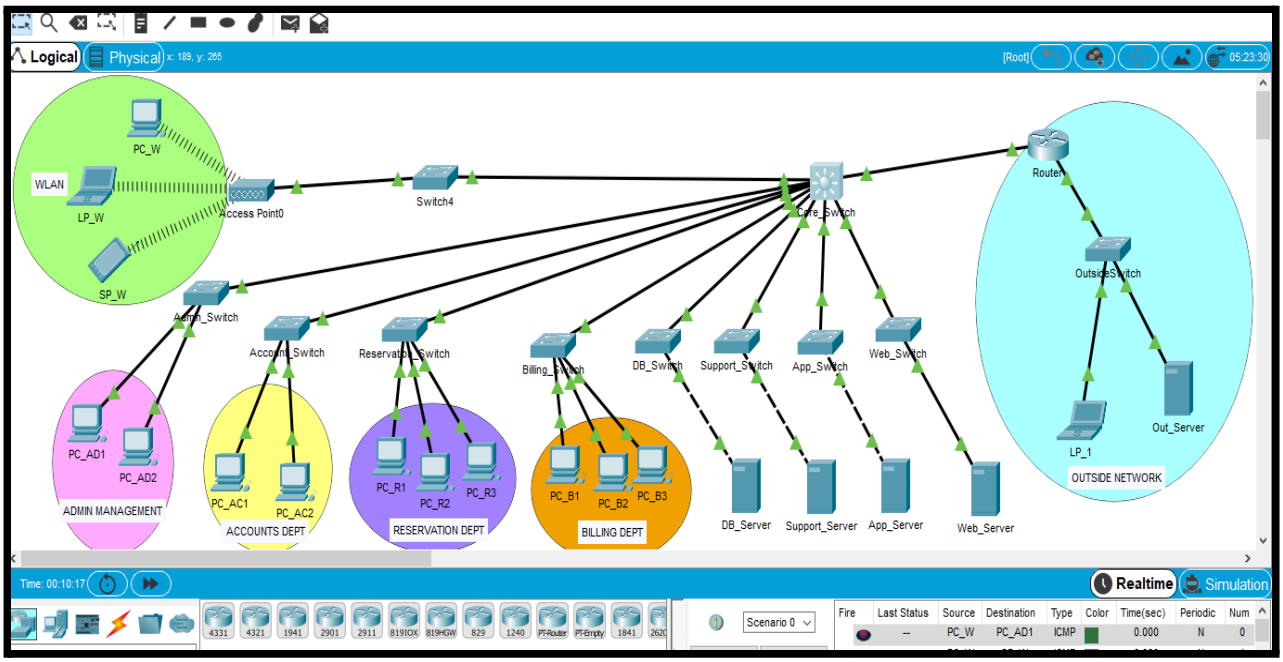

Figure-1: Complete Network Design

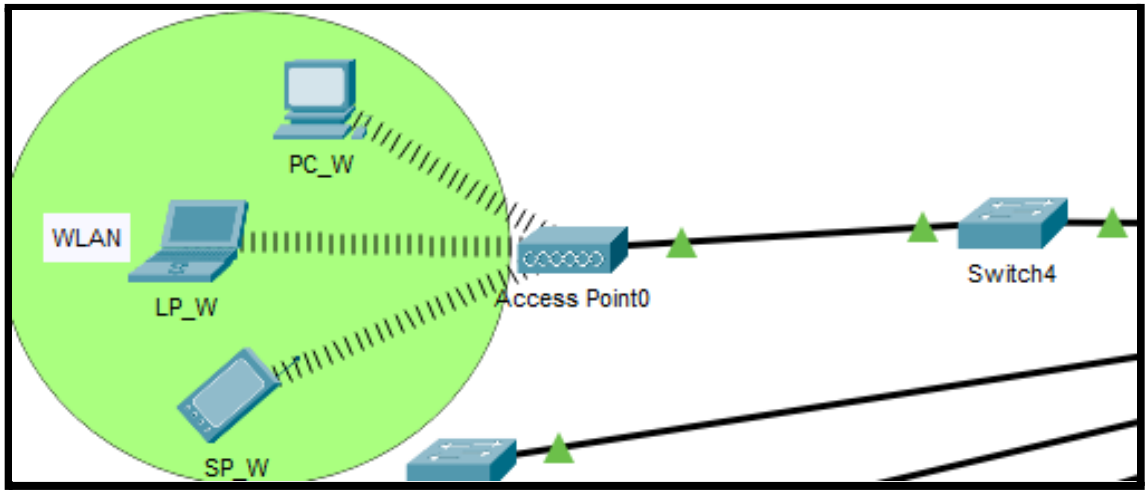

Figure-2: WLAN

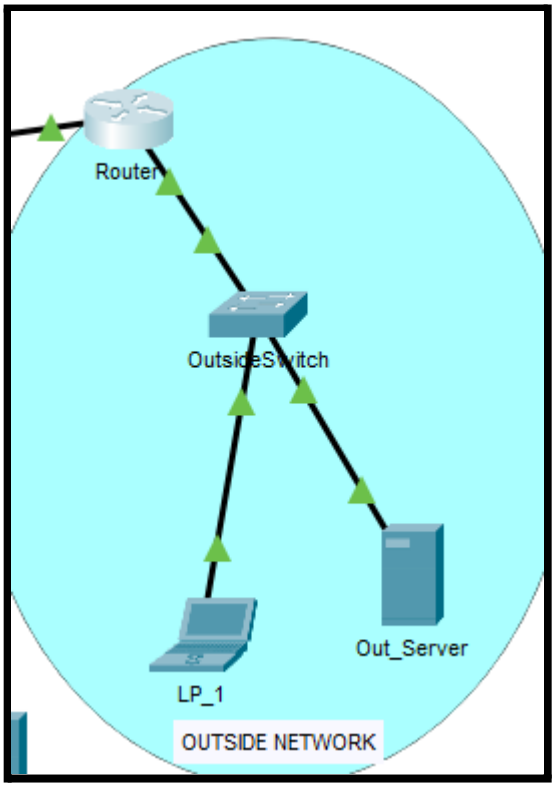

Figure-3: Outside Network

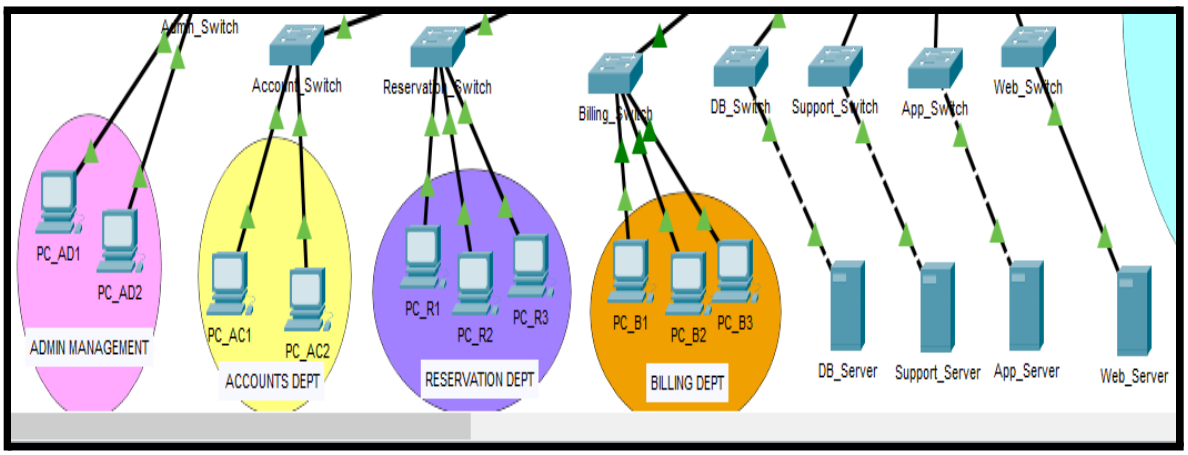

Figure-4: Inside Network

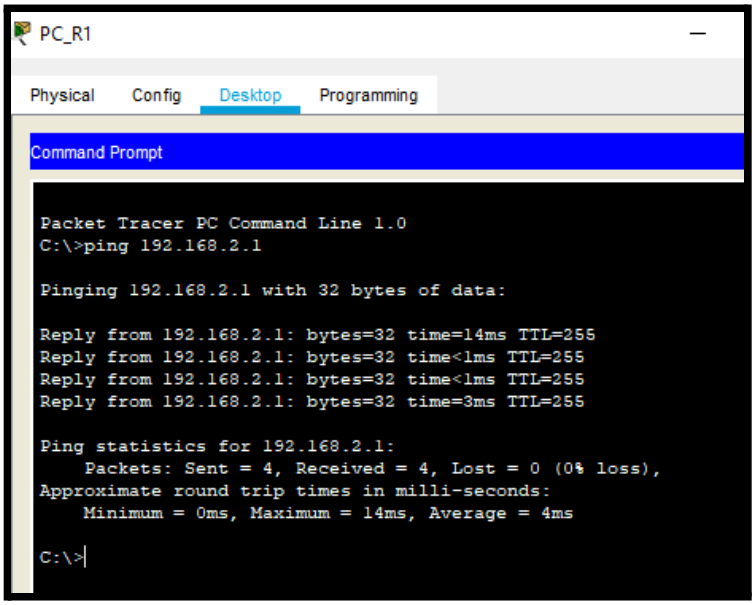

Figure-5: Pinging from Reservation Department PC - "PC -R1" to Admin Management PC- "PC_AD1"

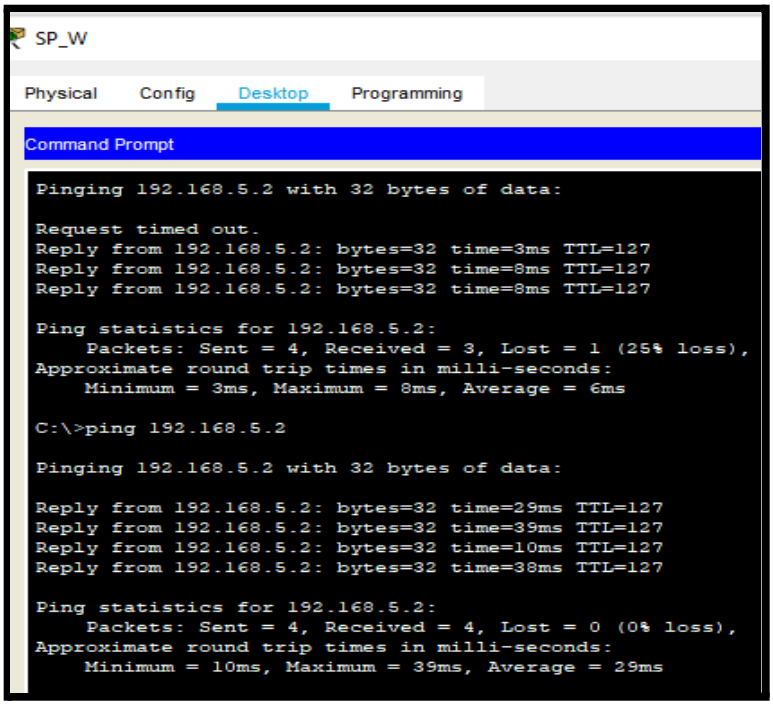

Figure-6: Pinging from WLAN Smart Device - "SP_W" to Billing Department PC- "PC_B1"

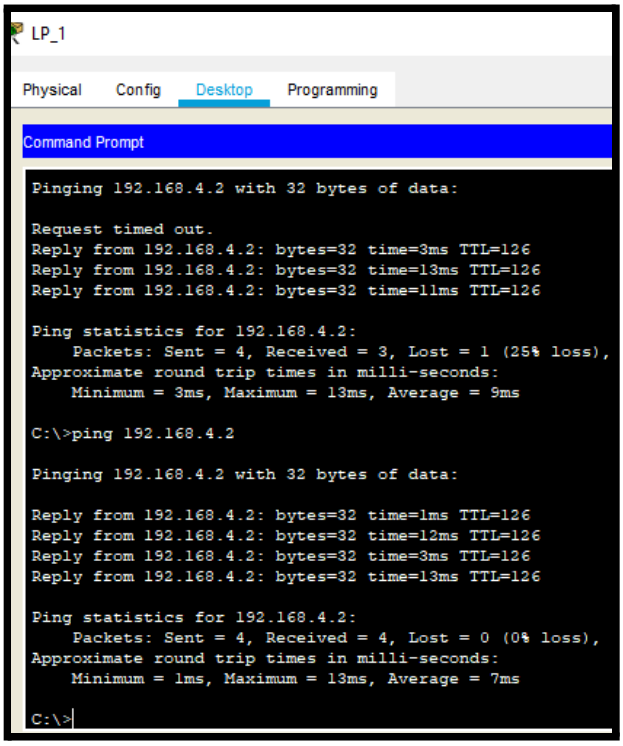

Figure-7: Pinging from Outside Network Laptop "LP_1" to Reservation Department PC - "PC-R1"

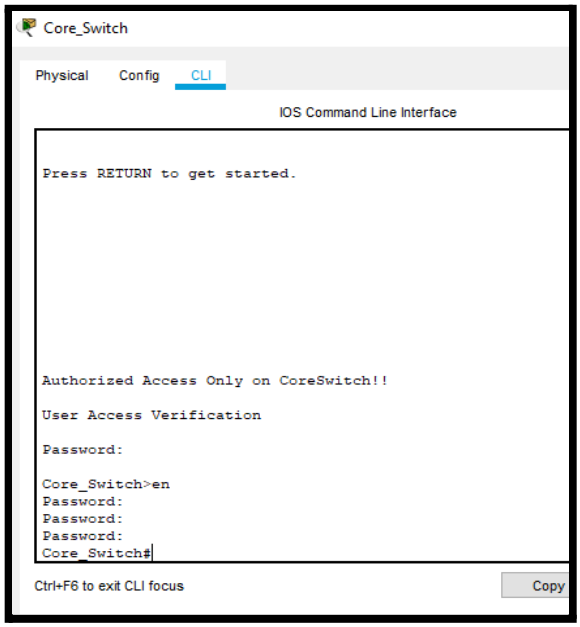

Figure-8: Basic Configuration

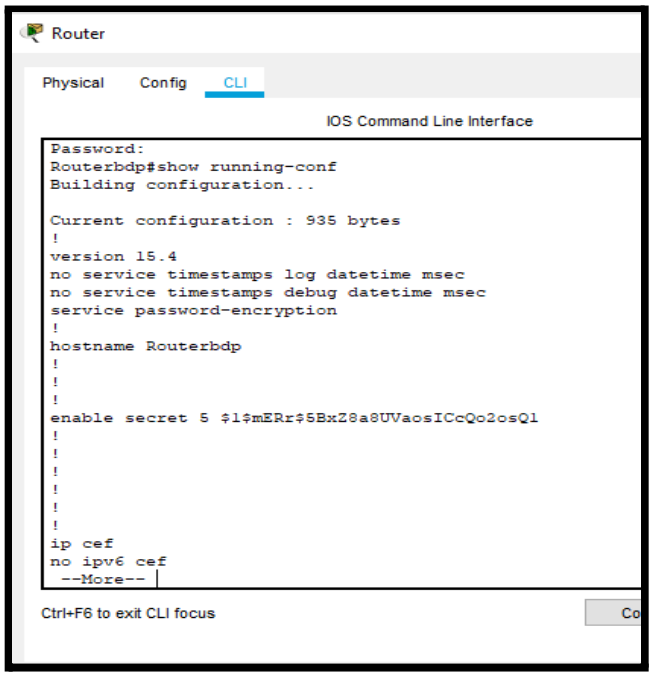

Figure-9: enable secret password

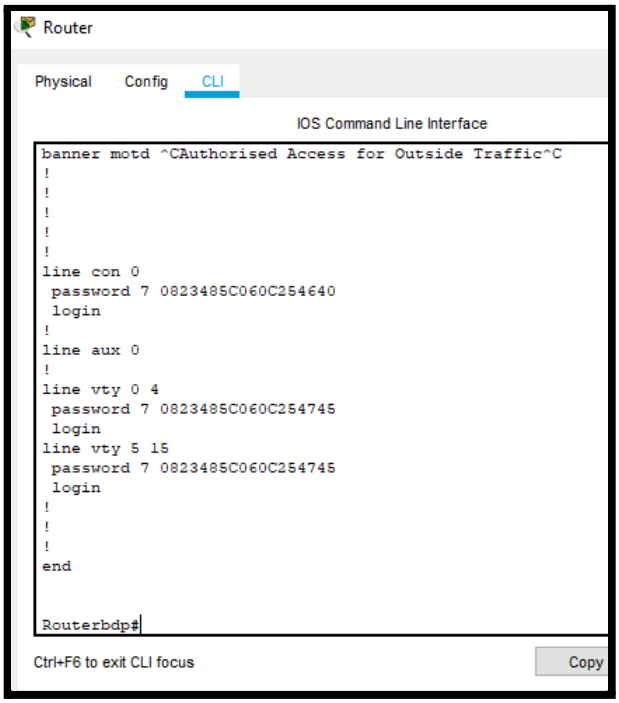

Figure-10: All password are encrypted

CONCLUSION

Network security is an important field that is getting more and more attention as the internet expands. The security threats and internet protocol should be analyzed to determine the necessary security technology. The security technology consists of mostly software based, as well as various hardware devices. In addition, network Security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access and the effectiveness (or lack) of these measures combined together.

REFERENCES

- www.netacad.com
- Fundamentals of Network Security

  - Eric Maiwald