

APPENDIX GA36d

LEVEL 7 ASSESSMENT SPECIFICATION

Student name:	ARYA MARTIN	Student ID number:	2220294
Programme:	Computer Networks and Cyber Security		
Module:	Network Security		
Module code:	ACCA7019	Contribution to Overall Module Assessment (%):	100%
Lecturer:	Dr Carlene Campbell	Internal Verifier:	Nitheesh Kaliyamurthy
Assignment Title:	Construct and mitigating security vulnerabilities and weaknesses.	Word count (or equivalent):	6,000
Submission deadline:	May 5 th 2023	Return date of provisional marks & written feedback:	
Submission method:	All written assessments, where practical and possible, must be submitted via Turnitin unless otherwise instructed by the Lecturer. (Please DO NOT put this assessment specification into Turnitin or it will match many similarities with other students' submissions.) Alternative submission method (if applicable): Late submission of the assessment will result in a late penalty mark. Penalties for late submission: Up to one week late, maximum mark of 50%. Over one week late, 0%. Only the Extenuating Circumstances Panel may approve a change to submission dates.		
Academic honesty / referencing:	Academic honesty is required. In the main body of your submission you must give credit to authors on whose research and ideas your work is based. Append to your submission a reference list that indicates the books, articles, etc. that you have used, cited or quoted in order to complete this assessment.		

Module Learning Outcomes (from module syllabus)
Provide a systematic understanding of a wide range of current research and technological advances in network security. Consistently apply the principles and practices of network security for mitigating the key technical internet security vulnerabilities that organisations face.

1. ABSTRACT

Over the past few years, organizations are dependent on their critical network infrastructure in order to make sure all business operations are carried out. The main purpose of this paper is to clearly provide explanation to all steps that were performed to complete network related tasks for secure configuration. All tasks are performed under the Cisco packet tracer simulation software and for each step, a screenshot with a detailed description is provided. In the second part of the report, a secure network blueprint is proposed to the A2Z organization that will aid in final network implementation. The proposal also includes costs, network vendor's analysis, timeline and even final cost for the secure network project.

2. TABLE OF CONTENTS

LEVEL 7 ASSESSMENT SPECIFICATION	1
1. Abstract	3
3. Introduction	8
4. Part 1: Laboratory Tasks Skill Set	9
4.1. Initial Configuration.....	10
4.2. Part 1: Questions/Answers	16
4.2.1. Network Security	16
4.2.2. Types of Threats and Attacks.....	16
4.2.3. Tools and Procedures	17
4.2.4. Fundamental Principles.....	17
4.2.5. Mitigations	17
4.2.6. Network Foundation Protection (NFP).....	18
4.2.7. Mitigations	18
4.2.8. End Point Vulnerabilities and Protection Methods	18
4.3. Part 2: Secure Cisco Routers.....	19
4.3.1. Secure Administrative Access.....	19
4.3.2. Privilege levels and role-based CLI	21
4.3.3. Secure Management and Monitoring	22
4.3.4. Automated Features	23
4.3.5. Control Plane Security.....	27

4.4. Part 3: AAA on Cisco Routers.....	28
4.4.1. AAA Explanation.....	28
4.4.2. Implement AAA authentication	28
4.4.3. Cisco Secure ACS	29
4.4.4. Server-based AAA Authentication.....	30
4.4.5. Server-based AAA Authorization and Accounting.....	31
4.5. Part 4: Mitigate threats using ACLs	32
4.5.1. Implement ACLs	32
4.5.2. Classic Firewall Configuration	33
4.5.3. Zone-Based Policy Firewall.....	34
4.6. Part 5: Implement Secure Network Design, Management and Reporting...	36
4.6.1. Implementation of a Comprehensive Security Policy	36
4.6.2. Techniques and tools for Network Security Testing	37
4.7. Part 6: Mitigate common Layer 2 attacks	37
4.7.1. Vulnerabilities and Mitigation techniques	37
4.7.2. Switch Security.....	38
4.8. Part 7: Implement the Cisco IOS firewall.....	41
4.8.1. Implement ACLs	41
4.8.2. Classic Firewall	42
4.8.3. Zone-Based Policy Firewall.....	42
4.9. Part 8: Implement the Cisco IOS IPS feature set	42

4.9.1. Network-based Intrusion Prevention Systems	42
4.9.2. Signatures Use	42
4.9.3. Configure Cisco IOS IPS operations	43
4.9.4. Verify Cisco IOS IPS operations	44
4.10.Part 9: Implement a site-to-site VPN.....	46
4.10.1.Purpose of VPNs.....	46
4.10.2.IPsec VPNs.....	47
4.10.3.Configure a site-to-site IPsec VPN	47
4.10.4.Description to Encryption, Hashes, and Digital Signatures for CIA.....	48
4.10.5.Use of Cryptographic hashes.....	48
4.10.6.Use of Encryption Algorithm	49
4.10.7.PKI Uses.....	49
4.11.Part 10: Implement a remote access VPN.....	50
4.11.1.Configure a Remote-access VPN	50
4.11.2.Configure Remote-access VPNs on an ASA	50
4.12.Part 11: Deploy the Cisco ASA for firewalling and NAT/PAT services.....	50
4.12.1.ASA Operating	50
4.12.2.Implementing ASA firewall	51
5. Part 2: Propose a secure network infrastructure	52
5.1. Introduction to the scenario	52
5.2. Network Blue Print	53

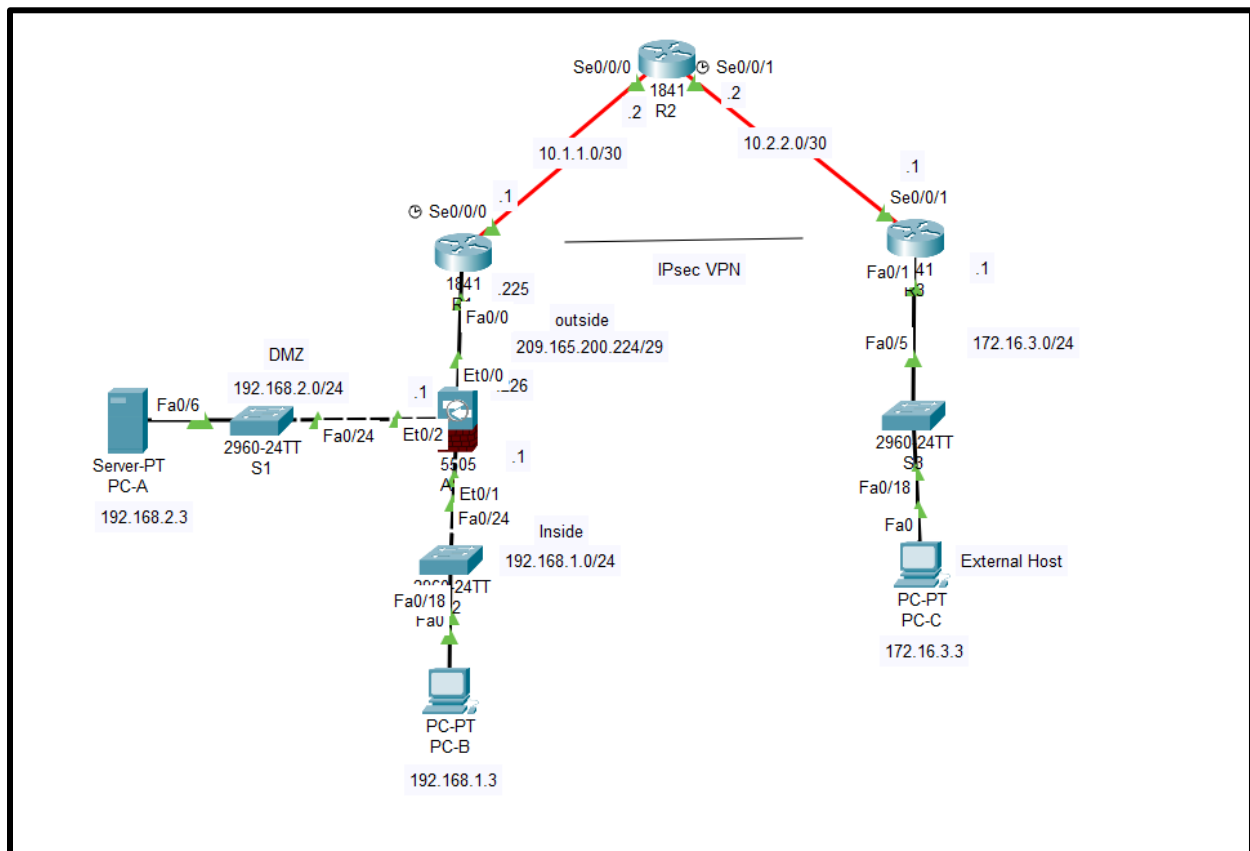
5.3. Justification of Network Design.....	54
5.4. Proposed Choices and Security Measures	55
5.5. Proposed Cost Analysis	57
5.5.1. Vendor 1.....	57
5.5.1. Vendor 2.....	59
5.7. Project Plan	61
5.8. Possible Attacks	62
5.9. Recommended Tests	63
5.10. Cost for Implementation	63
6. Conclusion	64
7. References	65

3. INTRODUCTION

The report provided here is divided into the two tasks, in the first task, there are questions about network security and some hands on labs that has to be performed in the Cisco Packet tracer. For each question and lab, a clear description is provided with respect to network configuration screenshots. Once the first part is completed, the next part is based on designing a secure network infrastructure for the A2Z Technology company. This network design is presented on the basis of technical and business needs in order to make sure all business operations are protected from all sort of cyber-attacks. It is also supported by the vendor comparison and a timeline that could be followed.

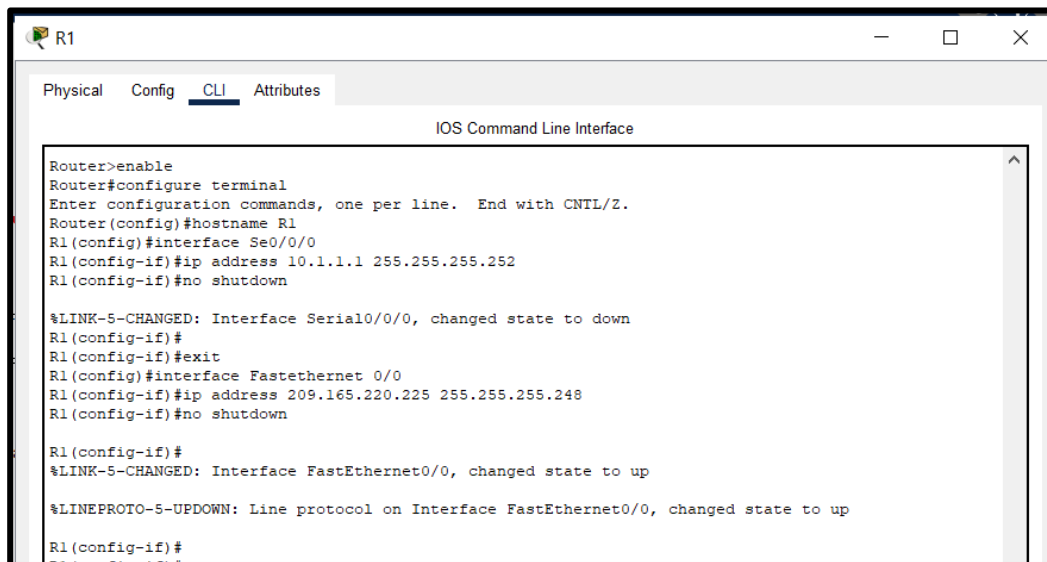
4. PART 1: LABORATORY TASKS SKILL SET

The first part is based on theoretical and practical tasks that needs to be done as per the given network configuration and IP addressing table. The below given network topology shows configuration of three routers while router R1 and R3 are communicating over IPsec VPN. At the first router site, a single switch is connected which further connects to a PC. On the other side, a router connects to a firewall; the first port is assigned to a DMZ switch and another switch is assigned to a host. The entire network has a single server placed under the DMZ zone which can be accessed by end hosts using public IP address.



4.1. INITIAL CONFIGURATION

On the basis of IP addressing scheme given above, the initial network configuration has been done. It starts from router R1 configuration that shows interface configuration such as serial interfaces and Fast Ethernet interfaces. All other routers are also configured in the proceeding screenshots (Sari et al., 2018).



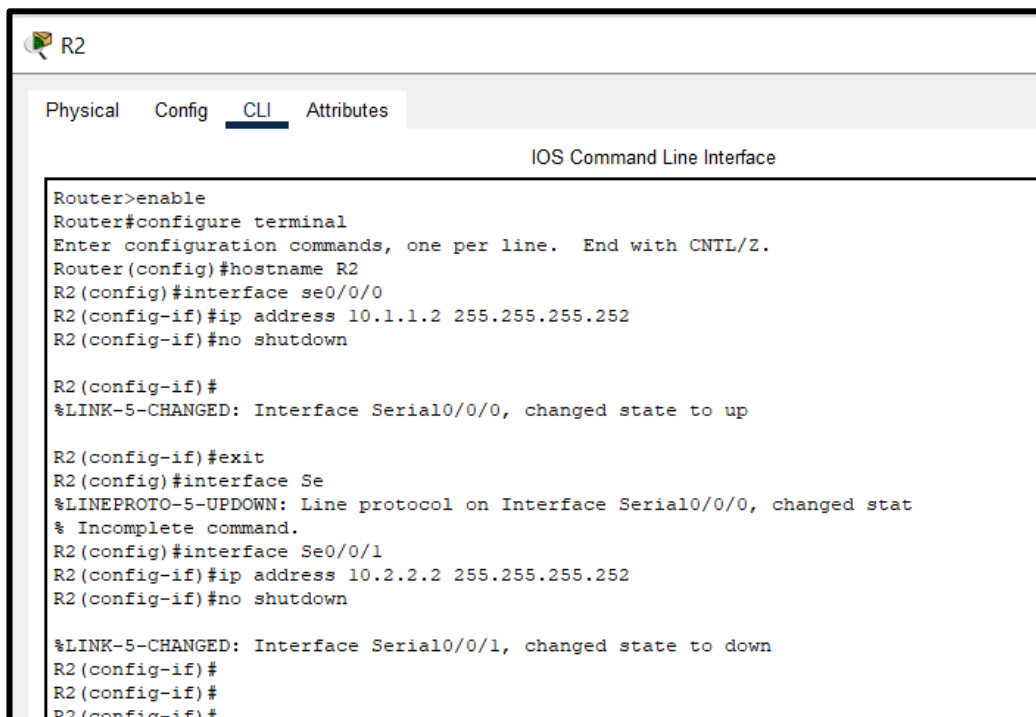
The screenshot shows the CLI of Router R1. The user has entered the following commands: `enable`, `configure terminal`, `hostname R1`, `interface Se0/0/0`, `ip address 10.1.1.1 255.255.255.252`, `no shutdown`, `exit`, `interface FastEthernet 0/0`, `ip address 209.165.220.225 255.255.255.248`, `no shutdown`, and `exit`. The system has responded with status messages: `%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down`, `%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up`, and `%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up`.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#interface Se0/0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#
R1(config-if)#exit
R1(config)#interface FastEthernet 0/0
R1(config-if)#ip address 209.165.220.225 255.255.255.248
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#
```



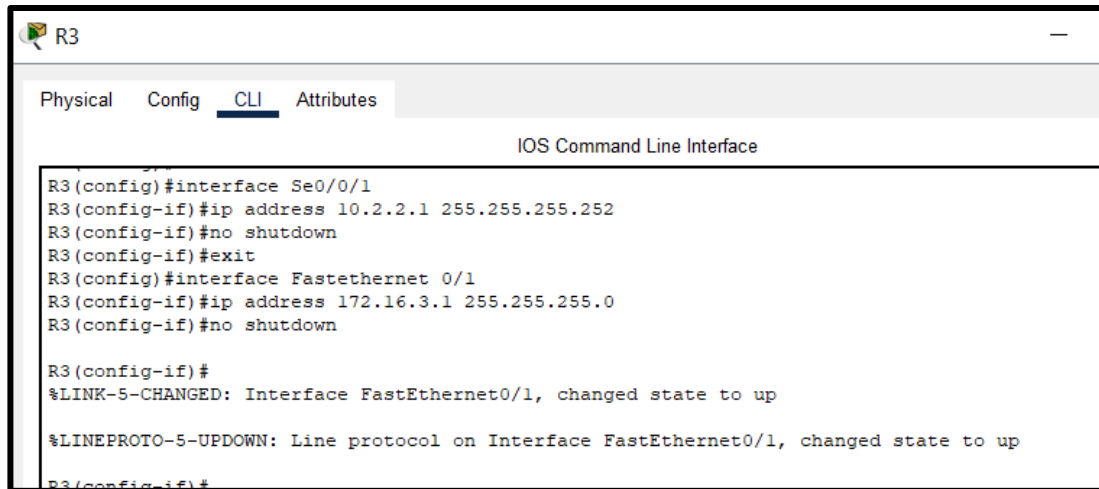
The screenshot shows the CLI of Router R2. The user has entered the following commands: `enable`, `configure terminal`, `hostname R2`, `interface se0/0/0`, `ip address 10.1.1.2 255.255.255.252`, `no shutdown`, `exit`, `interface Se`, `interface Se0/0/1`, `ip address 10.2.2.2 255.255.255.252`, `no shutdown`, and `exit`. The system has responded with status messages: `%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up`, `%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down`, and `%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down`.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#interface se0/0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R2(config-if)#exit
R2(config)#interface Se
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
% Incomplete command.
R2(config)#interface Se0/0/1
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#
R2(config-if)#
R2(config-if)#
```

A screenshot of the R3 router's CLI interface. The window title is 'R3'. At the top, there are tabs for 'Physical', 'Config', 'CLI' (which is selected), and 'Attributes'. Below the tabs, the text 'IOS Command Line Interface' is displayed. The main area shows the following commands and their outputs:

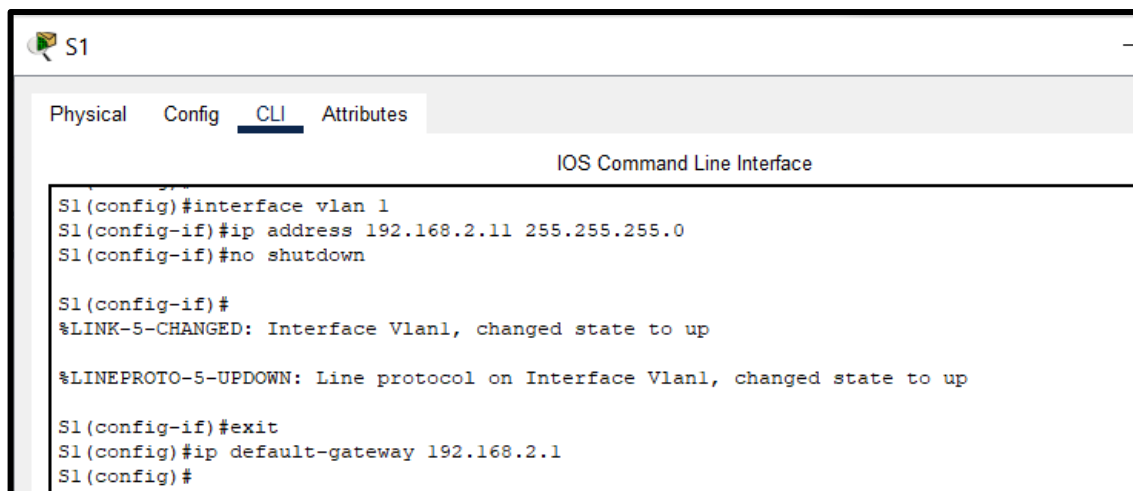
```
R3(config)#interface Se0/0/1
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface FastEthernet 0/1
R3(config-if)#ip address 172.16.3.1 255.255.255.0
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

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

R3(config-if)#
```

The switch connected to the network is also configured by assigning a VLAN 1, IP address, subnet mask and a gateway address (Sari et al., 2018).

A screenshot of the S1 switch's CLI interface. The window title is 'S1'. At the top, there are tabs for 'Physical', 'Config', 'CLI' (which is selected), and 'Attributes'. Below the tabs, the text 'IOS Command Line Interface' is displayed. The main area shows the following commands and their outputs:

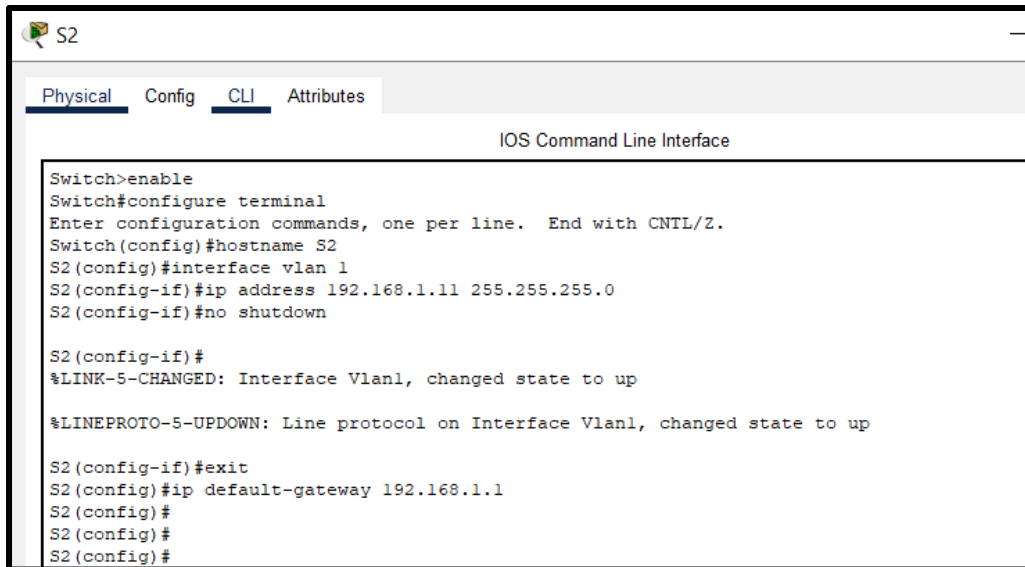
```
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.2.11 255.255.255.0
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#exit
S1(config)#ip default-gateway 192.168.2.1
S1(config)#
```

The second switch connected to the network is also assigned with VLAN ID, IP address, subnet mask and default gateway address.



The screenshot shows the CLI interface of a switch named S2. The tabs at the top are Physical, Config, CLI (selected), and Attributes. The title bar says 'S2'. The main window is titled 'IOS Command Line Interface'. The terminal output shows the following commands and responses:

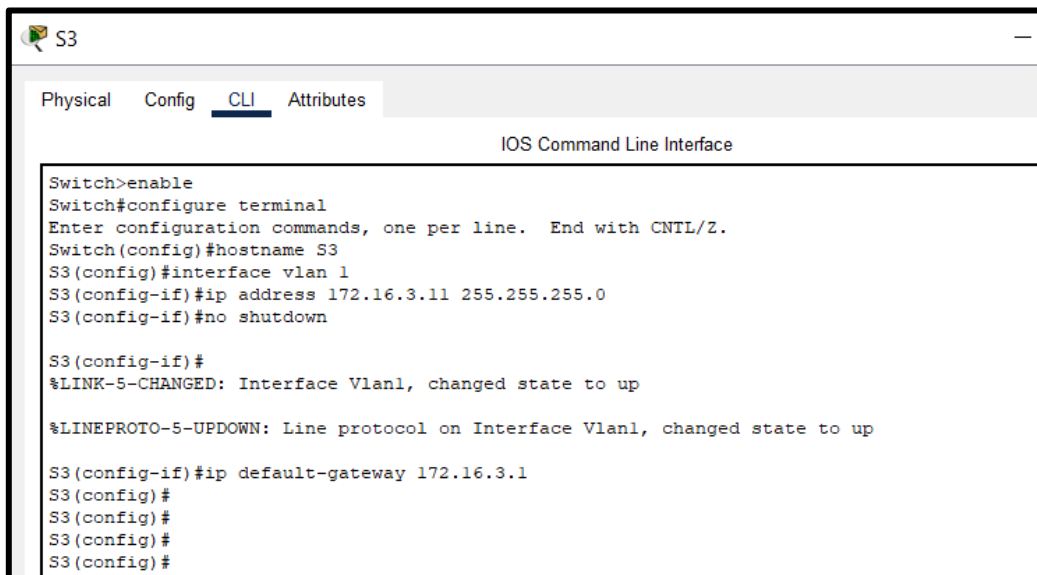
```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#interface vlan 1
S2(config-if)#ip address 192.168.1.11 255.255.255.0
S2(config-if)#no shutdown

S2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S2(config-if)#exit
S2(config)#ip default-gateway 192.168.1.1
S2(config)#
S2(config)#
S2(config)#
```

The last switch configured on the network also follows same configuration as switches 1 and 2.



The screenshot shows the CLI interface of a switch named S3. The tabs at the top are Physical, Config, CLI (selected), and Attributes. The title bar says 'S3'. The main window is titled 'IOS Command Line Interface'. The terminal output shows the following commands and responses:

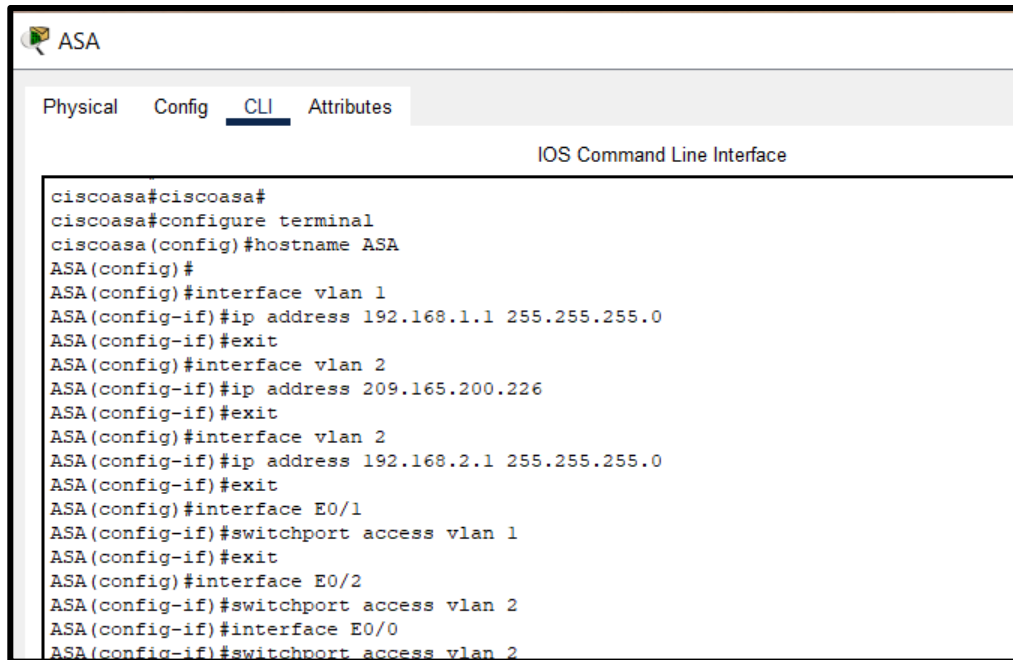
```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#interface vlan 1
S3(config-if)#ip address 172.16.3.11 255.255.255.0
S3(config-if)#no shutdown

S3(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

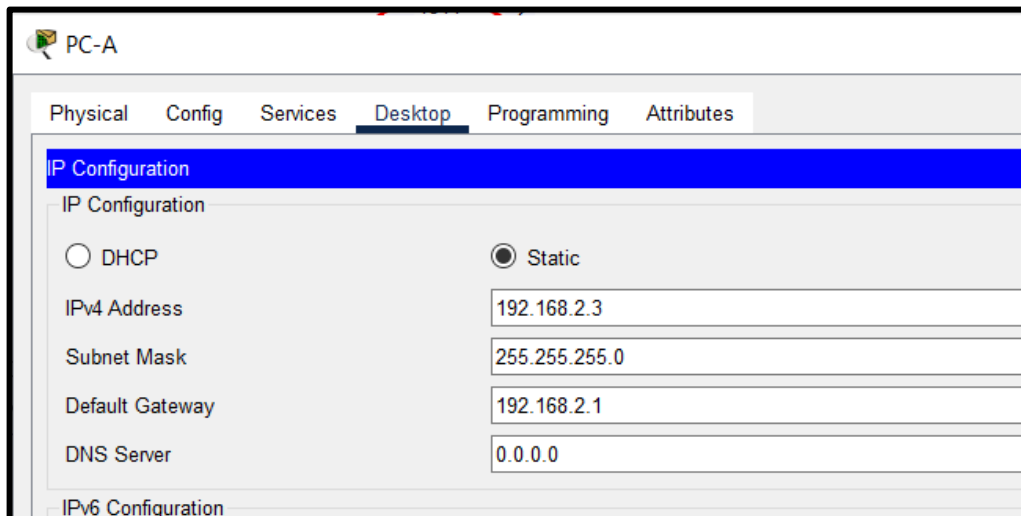
S3(config-if)#ip default-gateway 172.16.3.1
S3(config)#
S3(config)#
S3(config)#
S3(config)#
```

The hostname is allocated and all VLANs are registered which will remain protected from possible cyber threats.

A screenshot of the ASA (Cisco Adaptive Security Appliance) configuration window. The window has a title bar with a green icon and the text "ASA". Below the title bar is a tabbed interface with four tabs: "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is selected and highlighted. The main area of the window is titled "IOS Command Line Interface" and contains a text area with the following configuration commands:

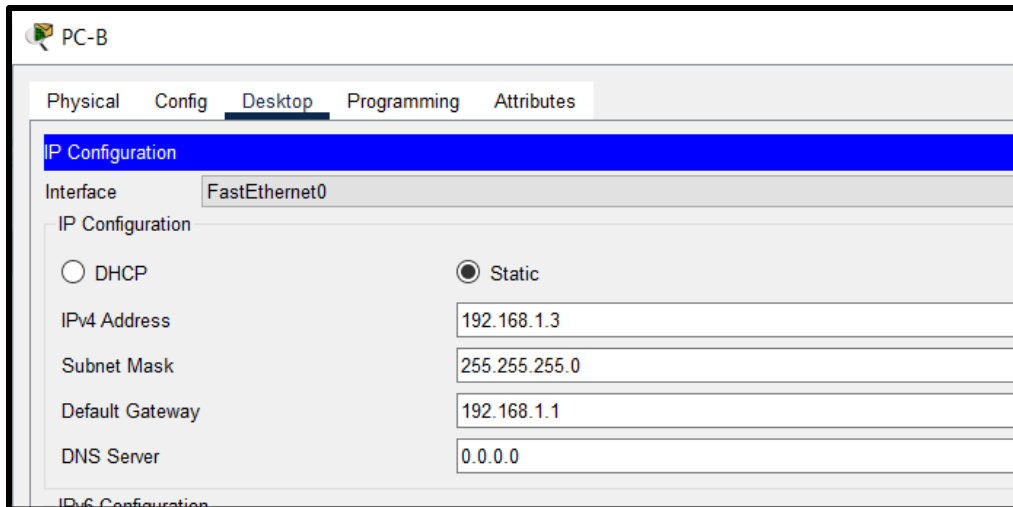
```
ciscoasa#ciscoasa#
ciscoasa#configure terminal
ciscoasa(config)#hostname ASA
ASA(config)#
ASA(config)#interface vlan 1
ASA(config-if)#ip address 192.168.1.1 255.255.255.0
ASA(config-if)#exit
ASA(config)#interface vlan 2
ASA(config-if)#ip address 209.165.200.226
ASA(config-if)#exit
ASA(config)#interface vlan 2
ASA(config-if)#ip address 192.168.2.1 255.255.255.0
ASA(config-if)#exit
ASA(config)#interface E0/1
ASA(config-if)#switchport access vlan 1
ASA(config-if)#exit
ASA(config)#interface E0/2
ASA(config-if)#switchport access vlan 2
ASA(config-if)#interface E0/0
ASA(config-if)#switchport access vlan 2
```

The PC-A is assigned with a static IP address as 192.168.2.3/255.255.255.0 (Sari et al., 2018).

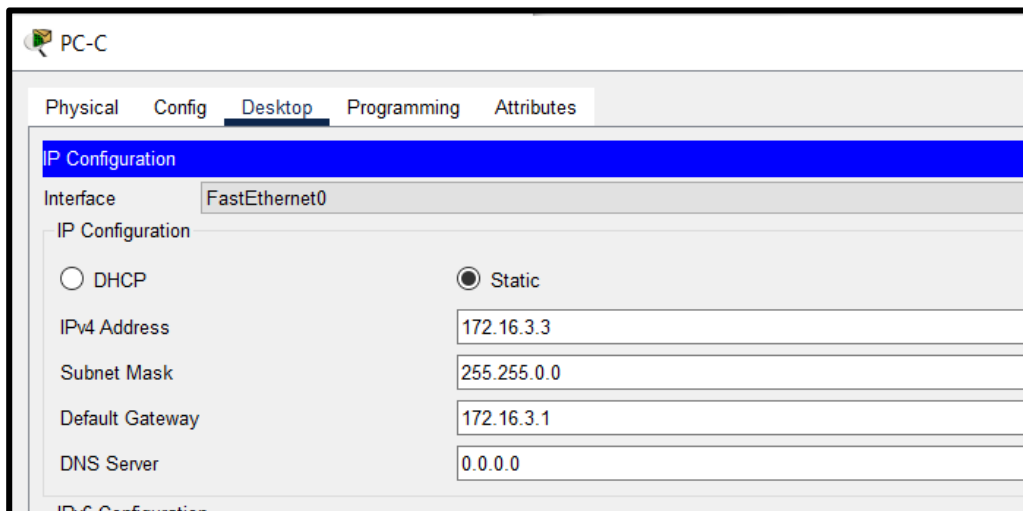
A screenshot of the PC-A configuration window, specifically the "Desktop" tab. The window has a title bar with a green icon and the text "PC-A". Below the title bar is a tabbed interface with five tabs: "Physical", "Config", "Services", "Desktop", and "Programming". The "Desktop" tab is selected and highlighted. The main area of the window is titled "IP Configuration" and contains a form for configuring the network settings. The "IP Configuration" section is expanded, showing options for "DHCP" and "Static". The "Static" option is selected with a radio button. Below this, there are input fields for "IPv4 Address", "Subnet Mask", "Default Gateway", and "DNS Server". The values entered are: IPv4 Address: 192.168.2.3, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.2.1, and DNS Server: 0.0.0.0. There is also a section for "IPv6 Configuration" which is currently collapsed.

IP Configuration	
☐ DHCP ☒ Static	
IPv4 Address	192.168.2.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server	0.0.0.0
IPv6 Configuration	

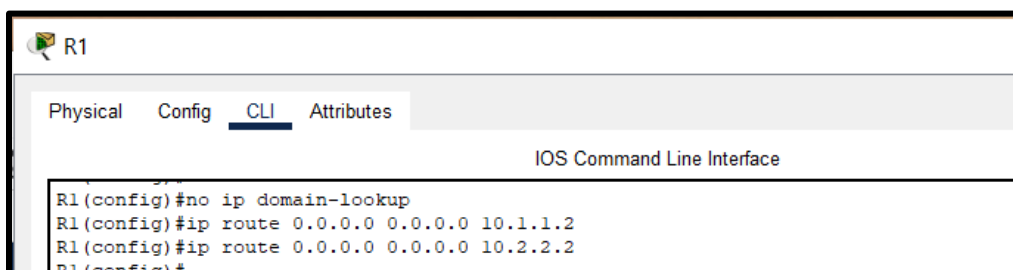
The PC-B is also assigned with a static IP address as 192.168.1.3/255.255.255.0.



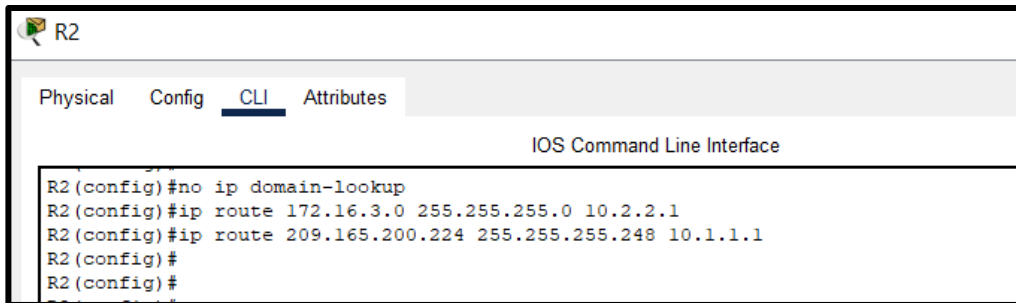
Lastly, for the PC-C also, the static IP address is assigned as 172.16.3.3/255.255.0.0.



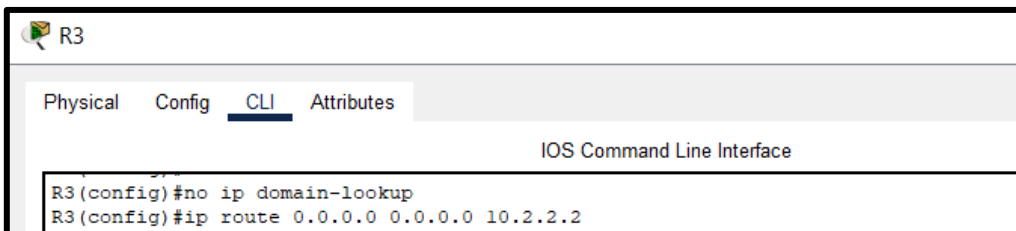
For the purpose of making router R1 operational, the IP domain look up command is executed and IP routes are added.



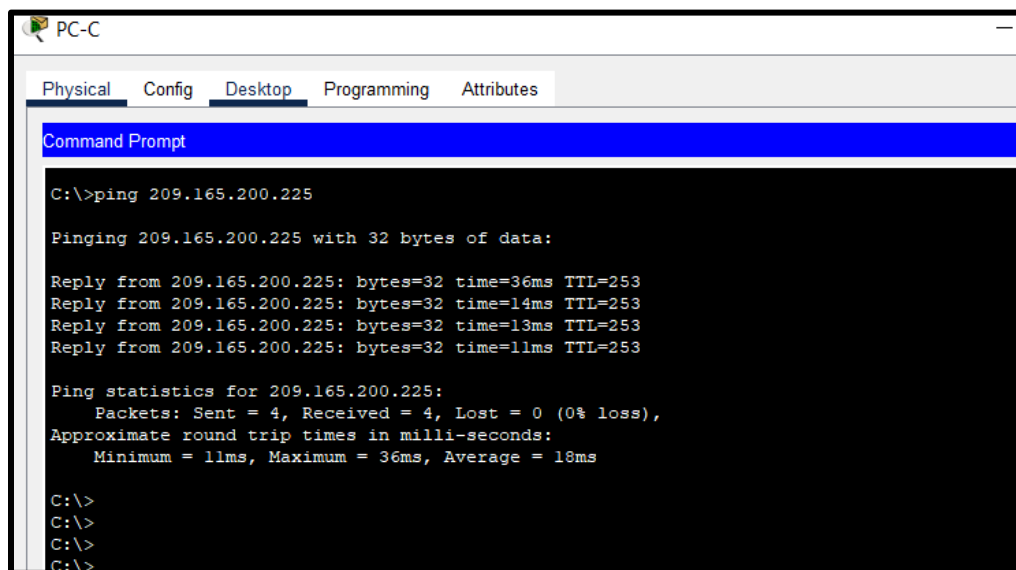
The same step is followed for the router R2.



For the router R3 also, same routing steps are followed.



Using the ping connectivity tool, network connectivity is checked between PC-C and 209.165.200.225.



4.2. PART 1: QUESTIONS/ANSWERS

4.2.1. Network Security

Network security entails protecting the computer networks from unauthorized access. The network security includes the various policies, procedures and many other technologies that can effectively protect the network. The network security also protects the network from the misuse of the resources from an unauthorized person. When there are proper network security mechanisms available, networks remain protected from possible cyber threats (Wang, Yu and Li, 2023).

4.2.2. Types of Threats and Attacks

Various types of threats and attacks that can cause breaches in the organizational network include malware attack, phishing, denial-of-service, man-in-the-middle and password based attacks. The first type of attack is malware based attack and it is designed in such a way that it can damage or disrupt the computer systems and could steal the sensitive information. Phishing, on the other hand, refers to an attack in which the attacker tries to trick the person to get the critical information such as details of the account, credit card details and passwords or usernames. Another major attack that could be faced on the network is distributed denial-of-service, a type of attack in which the attacker attempts to overload the server or a network with fake traffic to make network services unavailable to users. Another type of attack that is performed by cyber attackers is man-in-the-middle (MiTM) attack where the attacker tries to intercept the communication between the two people, allowing attackers to steal conversation data. Lastly, for password based attacks, these attacks are often conducted with the tools or the social engineering techniques which attempt to guess or crack the password of a user (Wang, Yu and Li, 2023).

4.2.3. Tools and Procedures

To mitigate the effect of the malware and other common network attacks, various kinds of tools like firewalls, intrusion detection systems, honey pot systems, security patches and updates could be used. The use of firewalls is done to block unauthorized access to the network and must only permit authorized users to access network services. Another type of security system that could be used is intrusion detection systems, to detect and prevent network attacks in real-time. Despite this system, the use of honey pot systems can also be done which can set up decoy network areas to catch cyber hackers easily. Moreover, the regular update of network devices and other protocols will also assure network remains up to date (Amal and Venkadesh, 2023).

4.2.4. Fundamental Principles

The fundamental principles of securing the network includes confidentiality, integrity, availability, authentication and authorization. Confidentiality means to ensure the critical information is kept safe from the attackers and is only accessible to the authorized users. Integrity refers to the accuracy of the data and also ensures that no one has altered the data. The availability ensures that the systems are available 24/7 wherever they are needed. Authentication verifies the users that are trying to access the network are genuine users or not. Authorization ensures that the user has the required permissions that are needed to access the network (Amal and Venkadesh, 2023).

4.2.5. Mitigations

The first step that the small to medium sized business can take to mitigate the effects of the common network attack methodologies is that they can regularly update their software so that the known vulnerabilities can be fixed. Another step is that they can implement the strong passwords and the policies of security and also

update them when required. They can also implement the firewalls and the other security measures that can help them to block the access of the unauthorized user. They can also backup the data on a regular basis to ensure the security of the data.

4.2.6. Network Foundation Protection (NFP)

The Cisco Network Foundation Protection (NFP) framework is used to secure a network by providing a multiple layer of defense which includes control plane protection, data plane protection and management plane protection. Control plane protection is protecting the network by detecting and mitigating the attacks over the network. The control plane also blocks unauthorized access on the network. The other protection layer is the data plane protection, which controls the overall access of the users to the resources (Wu, Qi and Yu, 2023).

4.2.7. Mitigations

To mitigate the effects of Viruses, Worms and Trojan Horses in a small to medium business can regularly update their software and firmware so that the known vulnerability can be fixed as early as possible. Secondly, they can implement the firewalls and the other security measures to prevent the network from unauthorized access. They can also provide the training to their employees so that they can be aware of the latest scams and attacks over the network. They can also use the backup options to back up their data and store it in a secure location.

4.2.8. End Point Vulnerabilities and Protection Methods

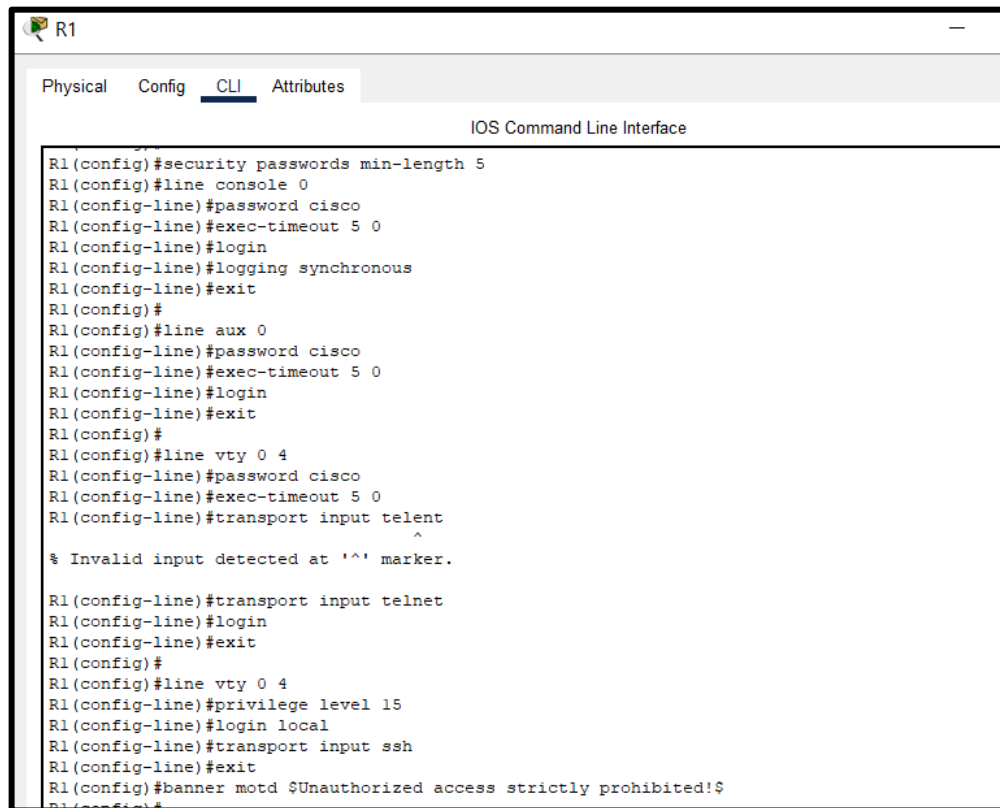
Endpoint vulnerabilities are the vulnerabilities that are found in individual devices like laptops, smartphones, etc. to protect the endpoint vulnerability one must update the security patches regularly to prevent any malware attack. Another way to prevent the endpoint vulnerability is the BYOD (Bring Your Own Device) policy. By implementing this policy one can determine the limited apps and the

devices over a network to provide a secure environment to the user (Wu, Qi and Yu, 2023).

4.3. PART 2: SECURE CISCO ROUTERS

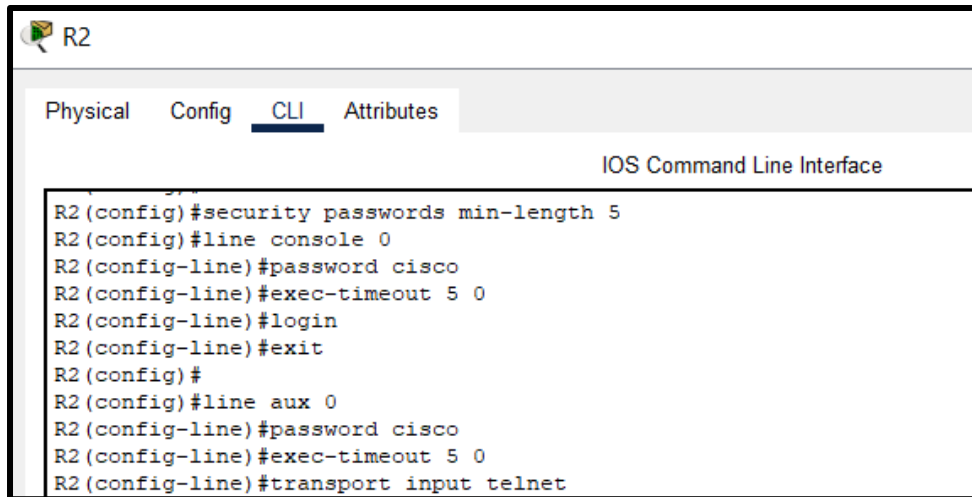
4.3.1. Secure Administrative Access

For the purpose of setting up secure administrative access, there is a need for following some steps such as password length, synchronous login, password and privileges level. All these settings are done on the router R1 as shown in the screenshot attached below.



```
R1
Physical Config CLI Attributes
IOS Command Line Interface
R1(config)#security passwords min-length 5
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#
R1(config)#line aux 0
R1(config-line)#password cisco
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#exec-timeout 5 0
R1(config-line)#transport input telnet
R1(config-line)#transport input telnet
^
% Invalid input detected at '^' marker.
R1(config-line)#transport input telnet
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#line vty 0 4
R1(config-line)#privilege level 15
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#banner motd $Unauthorized access strictly prohibited!$
R1(config)#
```

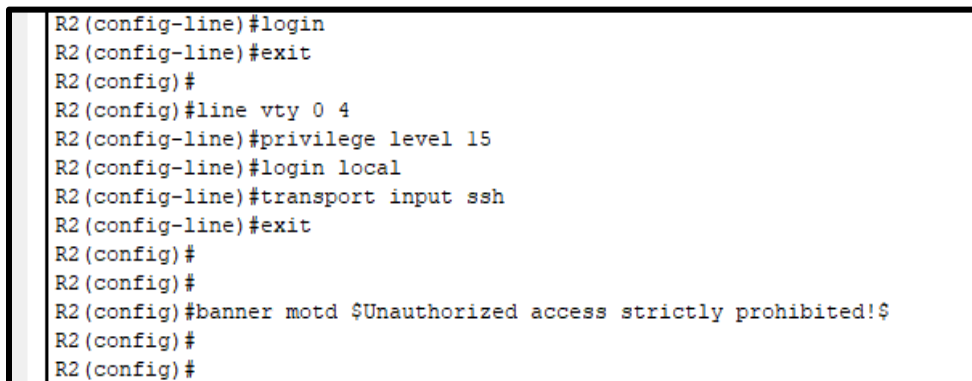
For the router R2 configuration, the security password length is assigned for the line console and password is set for the line aux as shown below.



The screenshot shows the R2 CLI interface with the 'CLI' tab selected. The 'IOS Command Line Interface' section displays the following configuration commands:

```
R2(config)#security passwords min-length 5
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#exec-timeout 5 0
R2(config-line)#login
R2(config-line)#exit
R2(config)#
R2(config)#line aux 0
R2(config-line)#password cisco
R2(config-line)#exec-timeout 5 0
R2(config-line)#transport input telnet
```

In addition to this, login is made and privilege level 15 is assigned to the line VTY despite using SSH for transportation.



The screenshot shows the R2 CLI interface with the following configuration commands:

```
R2(config-line)#login
R2(config-line)#exit
R2(config)#
R2(config)#line vty 0 4
R2(config-line)#privilege level 15
R2(config-line)#login local
R2(config-line)#transport input ssh
R2(config-line)#exit
R2(config)#
R2(config)#
R2(config)#banner motd $Unauthorized access strictly prohibited!$
R2(config)#
R2(config)#
```

In the case of router R3 also, the same configuration has been followed to set up secure configurations for the router (Xiong et al., 2023).

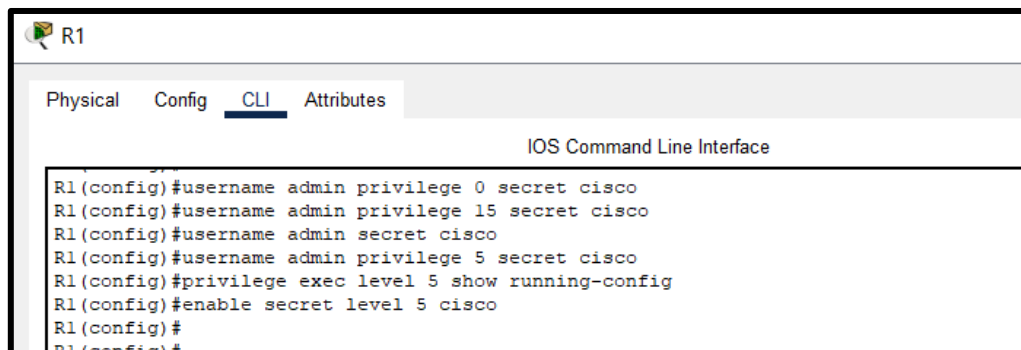
A screenshot of a network simulator interface for router R3. The top bar shows tabs for Physical, Config, CLI (selected), and Attributes. Below the tabs is the title 'IOS Command Line Interface'. The main area displays a series of configuration commands entered in the CLI. The commands configure security passwords, console and aux lines, and vty lines with various settings like login, logging, and transport input.

```
R3
Physical Config CLI Attributes
IOS Command Line Interface

R3(config)#security passwords min-length 5
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#exec-timeout 5 0
R3(config-line)#login
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#
R3(config)#line aux 0
R3(config-line)#password cisco
R3(config-line)#exec-timeout 5 0
R3(config-line)#login
R3(config-line)#exit
R3(config)#
R3(config)#
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#exec-timeout 5 0
R3(config-line)#transport input telnet
R3(config-line)#login
R3(config-line)#exit
R3(config)#
R3(config)#line vty 0 4
R3(config-line)#privilege level 15
R3(config-line)#login local
R3(config-line)#transport input ssh
R3(config-line)#exit
R3(config)#
```

4.3.2. Privilege levels and role-based CLI

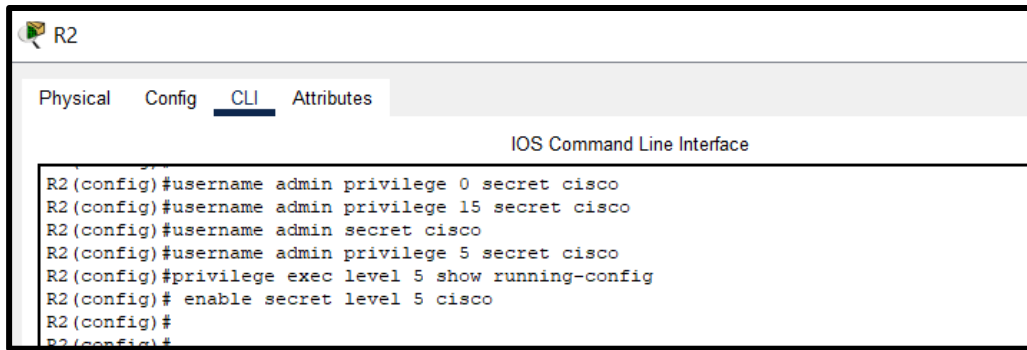
After secure administrative access, the next set is to set up privilege levels and roles on the basis of CLI. In the screenshot attached below, the administrator is assigned with privileges along with different roles.

A screenshot of a network simulator interface for router R1. The top bar shows tabs for Physical, Config, CLI (selected), and Attributes. Below the tabs is the title 'IOS Command Line Interface'. The main area displays a series of configuration commands entered in the CLI. The commands configure usernames with different privilege levels and enable the 'show running-config' command at privilege level 5.

```
R1
Physical Config CLI Attributes
IOS Command Line Interface

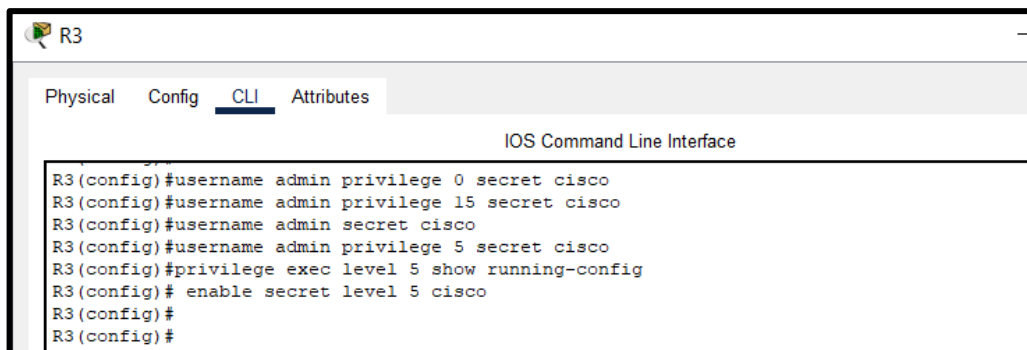
R1(config)#username admin privilege 0 secret cisco
R1(config)#username admin privilege 15 secret cisco
R1(config)#username admin secret cisco
R1(config)#username admin privilege 5 secret cisco
R1(config)#privilege exec level 5 show running-config
R1(config)#enable secret level 5 cisco
R1(config)#
```

In the case of router R2 also, the administrator is assigned with privileges and roles to access network.

A screenshot of the Cisco Packet Tracer interface for router R2. The 'CLI' tab is selected under the 'Config' menu. The command prompt shows the following configuration commands: R2(config)#username admin privilege 0 secret cisco, R2(config)#username admin privilege 15 secret cisco, R2(config)#username admin secret cisco, R2(config)#username admin privilege 5 secret cisco, R2(config)#privilege exec level 5 show running-config, R2(config)# enable secret level 5 cisco, R2(config)#, and R2(config)#.

```
R2
Physical Config CLI Attributes
IOS Command Line Interface
R2(config)#username admin privilege 0 secret cisco
R2(config)#username admin privilege 15 secret cisco
R2(config)#username admin secret cisco
R2(config)#username admin privilege 5 secret cisco
R2(config)#privilege exec level 5 show running-config
R2(config)# enable secret level 5 cisco
R2(config)#
R2(config)#
```

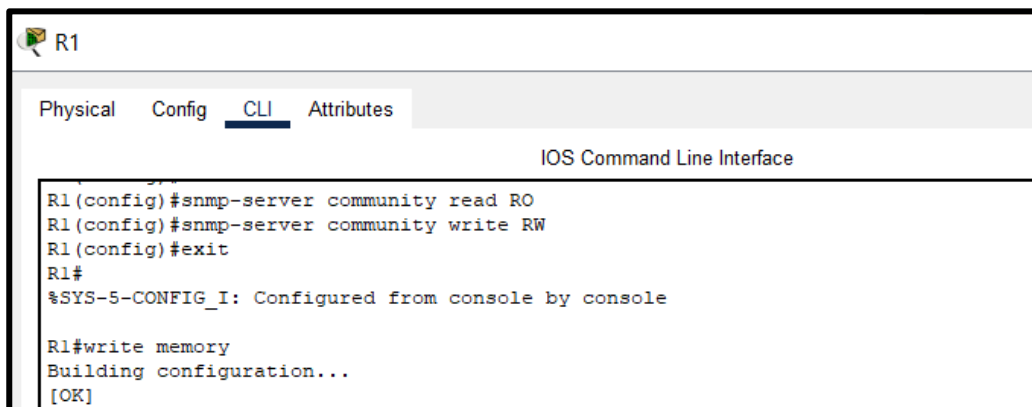
The same configuration options have been used for the router R3 also as shown in the screenshot below.

A screenshot of the Cisco Packet Tracer interface for router R3. The 'CLI' tab is selected under the 'Config' menu. The command prompt shows the following configuration commands: R3(config)#username admin privilege 0 secret cisco, R3(config)#username admin privilege 15 secret cisco, R3(config)#username admin secret cisco, R3(config)#username admin privilege 5 secret cisco, R3(config)#privilege exec level 5 show running-config, R3(config)# enable secret level 5 cisco, R3(config)#, and R3(config)#.

```
R3
Physical Config CLI Attributes
IOS Command Line Interface
R3(config)#username admin privilege 0 secret cisco
R3(config)#username admin privilege 15 secret cisco
R3(config)#username admin secret cisco
R3(config)#username admin privilege 5 secret cisco
R3(config)#privilege exec level 5 show running-config
R3(config)# enable secret level 5 cisco
R3(config)#
R3(config)#
```

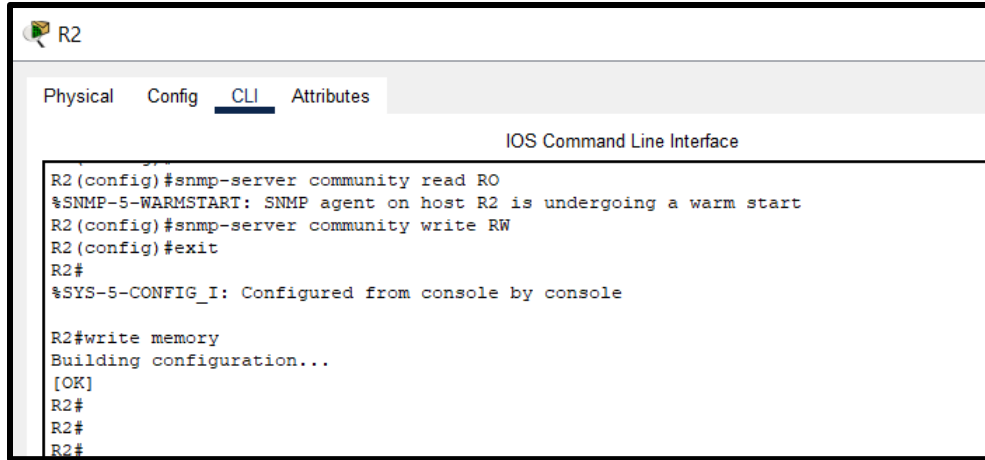
4.3.3. Secure Management and Monitoring

For the purpose of secure management and monitoring, the SNMP server is set to read/write permissions and configuration is saved.

A screenshot of the Cisco Packet Tracer interface for router R1. The 'CLI' tab is selected under the 'Config' menu. The command prompt shows the following configuration commands: R1(config)#snmp-server community read RO, R1(config)#snmp-server community write RW, R1(config)#exit, R1#, %SYS-5-CONFIG_I: Configured from console by console, R1#write memory, Building configuration..., and [OK].

```
R1
Physical Config CLI Attributes
IOS Command Line Interface
R1(config)#snmp-server community read RO
R1(config)#snmp-server community write RW
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#write memory
Building configuration...
[OK]
```

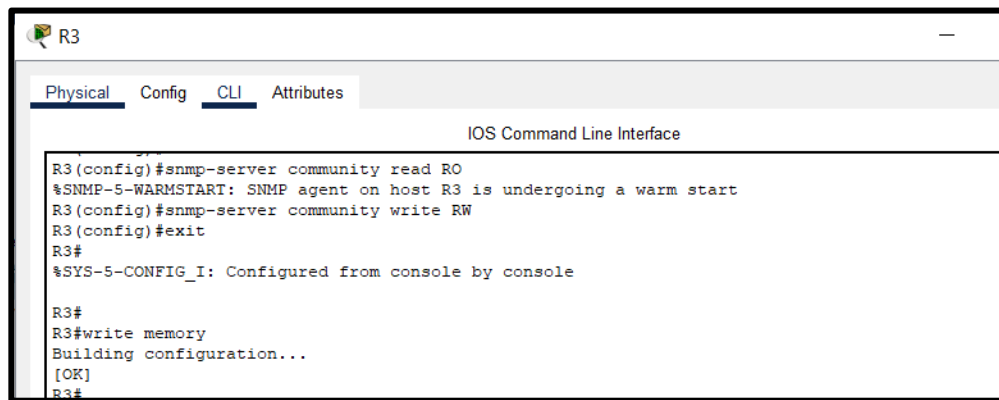
In the case of router R2 also, the agent is enabled and read and write operations are assigned.

A screenshot of the R2 router's CLI interface. The window has tabs for Physical, Config, CLI (selected), and Attributes. The title bar says "R2". The main area is titled "IOS Command Line Interface" and contains the following text:

```
R2(config)#snmp-server community read RO
%SNMP-5-WARMSTART: SNMP agent on host R2 is undergoing a warm start
R2(config)#snmp-server community write RW
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#write memory
Building configuration...
[OK]
R2#
R2#
R2#
```

Finally, for the router R3, the same configuration steps have been followed and configuration is saved to the memory (Xiong et al., 2023).

A screenshot of the R3 router's CLI interface. The window has tabs for Physical, Config, CLI (selected), and Attributes. The title bar says "R3". The main area is titled "IOS Command Line Interface" and contains the following text:

```
R3(config)#snmp-server community read RO
%SNMP-5-WARMSTART: SNMP agent on host R3 is undergoing a warm start
R3(config)#snmp-server community write RW
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#
R3#write memory
Building configuration...
[OK]
R3#
```

4.3.4. Automated Features

In the screenshot attached below, the router R1 console is opened and auto secure command is executed.

```
R1
Physical Config CLI Attributes
IOS Command Line Interface

R1#auto secure

--- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
AutoSecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: yes
Enter the number of interfaces facing the internet [1]: se0/0/0
% A decimal number between 1 and 2147483647.
Enter the number of interfaces facing the internet [1]: 1
Interface      IP-Address      OK? Method Status          Protocol
FastEthernet0/0 209.165.200.225 YES manual up             up
FastEthernet0/1 unassigned      YES unset  administratively down down
Serial0/0/0     10.1.1.1        YES manual up             up
Serial0/0/1     unassigned      YES unset  administratively down down
Vlan1           unassigned      YES unset  administratively down down

Enter the interface name that is facing the internet: serial0/0/0

Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
```

The final list of all auto secure parameters performed by the IOS console are shown below.

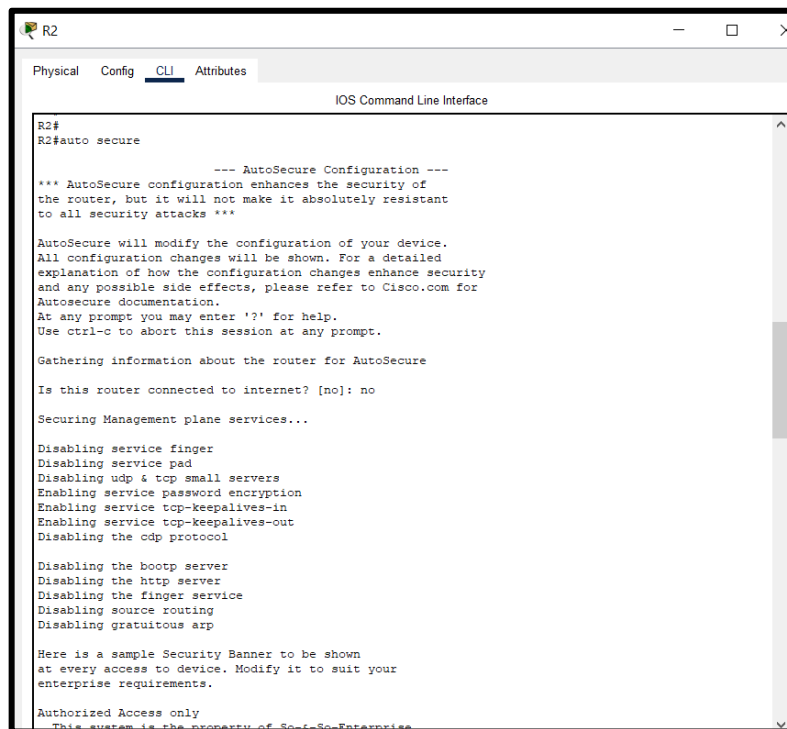
```
IOS Command Line Interface

exec-timeout 5 0
transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
service timestamps debug datetime msec
service timestamps log datetime msec
logging trap debugging
logging console
logging buffered
line vty 0 4
 transport input ssh
 transport input telnet
hostname R1
ip domain-name R1
ip access-list extended 100
 permit udp any any eq bootpc
ip inspect audit-trail
ip inspect dns-timeout 7
ip inspect tcp idle-time 14400
ip inspect udp idle-time 1800
ip inspect name autosec_inspect http timeout 3600
ip inspect name autosec_inspect udp timeout 15
ip inspect name autosec_inspect tcp timeout 3600
ip access-list extended autosec_firewall_acl
 permit udp any any eq bootpc
 deny ip any any
interface Serial0/0/0
 ip inspect autosec_inspect out
 ip access-group autosec_firewall_acl in

Apply this configuration to running-config? [yes]: yes
Applying the config generated to running-config
The name for the keys will be: test.test

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
*Mar 1 22:56:41.001: %SYS-3-CPUHOG: Task is running for (2007)msecs, more than
(2000)msecs (0/0),process = crypto sw pk proc.
-Traceback= 0x824198E0 0x82419FC4 0x8283C238 0x82866AD8 0x828667A8 0x82865D34 0x
828660F4 0x82866510 0x802335D4 0x80236D80 [OK]
R1#
```

In the case of router R2 also, the auto secure command is executed which automatically secures router R2 from getting impacted.



```
R2#
R2#auto secure

--- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
AutoSecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: no

Securing Management plane services...

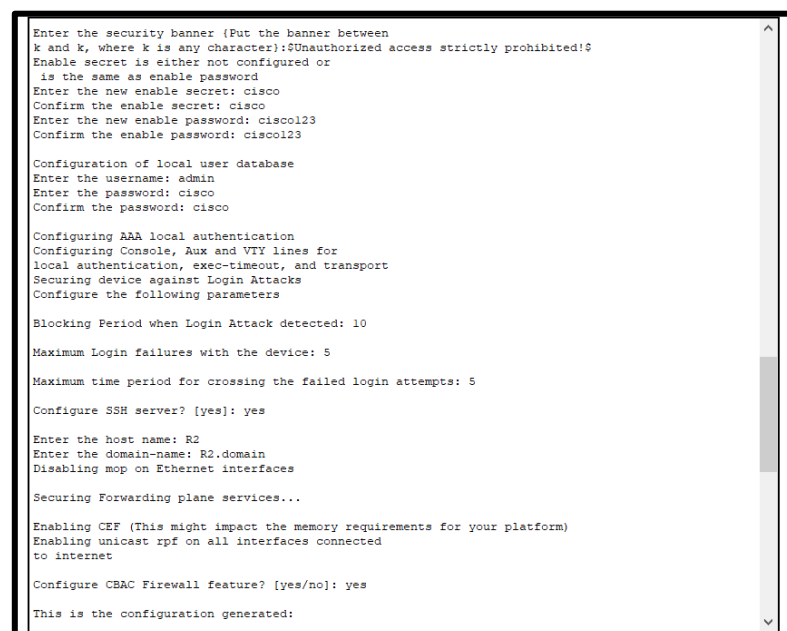
Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp

Here is a sample Security Banner to be shown
at every access to device. Modify it to suit your
enterprise requirements.

Authorized Access only
This system is the property of Soft-Sol-Enterprise
```

The auto secure configuration for the router R2 is now completed.



```
Enter the security banner (Put the banner between
k and k, where k is any character):$Unauthorized access strictly prohibited!$
Enable secret is either not configured or
is the same as enable password
Enter the new enable secret: cisco
Confirm the enable secret: cisco
Enter the new enable password: cisco123
Confirm the enable password: cisco123

Configuration of local user database
Enter the username: admin
Enter the password: cisco
Confirm the password: cisco

Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: 10

Maximum Login failures with the device: 5

Maximum time period for crossing the failed login attempts: 5

Configure SSH server? [yes]: yes

Enter the host name: R2
Enter the domain-name: R2.domain
Disabling mop on Ethernet interfaces

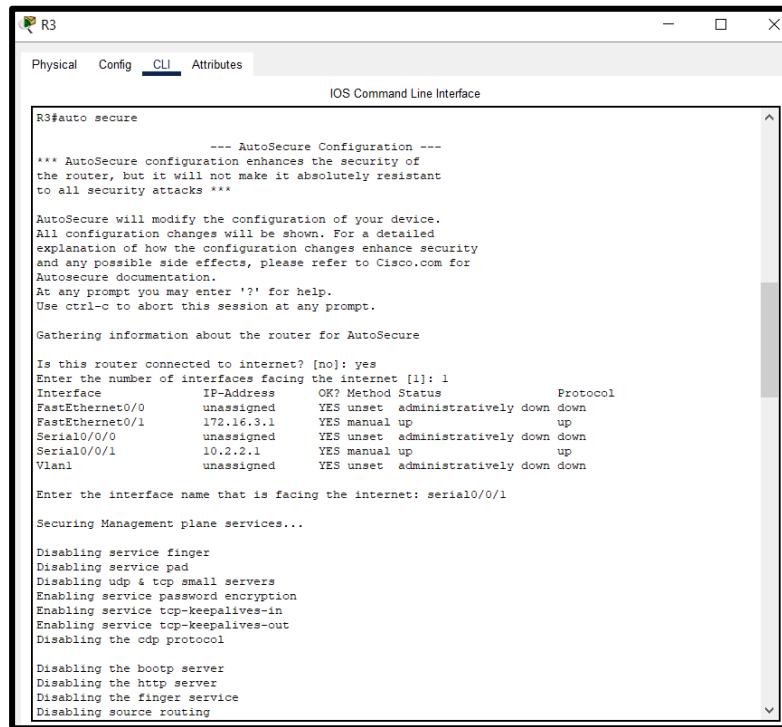
Securing Forwarding plane services...

Enabling CEF (This might impact the memory requirements for your platform)
Enabling unicast rpf on all interfaces connected
to internet

Configure CBAC Firewall feature? [yes/no]: yes

This is the configuration generated:
```

Lastly, for the router R3 also, the auto secure command is executed that will secure router from any misconfigurations (Xiong et al., 2023).



```
R3#auto secure

--- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
AutoSecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: yes
Enter the number of interfaces facing the internet [1]: 1
Interface      IP-Address      OK? Method Status      Protocol
FastEthernet0/0 unassigned      YES unset   administratively down down
FastEthernet0/1 172.16.3.1      YES manual   up           up
Serial0/0/0      unassigned      YES unset   administratively down down
Serial0/0/1      10.2.2.1        YES manual   up           up
Vlan1            unassigned      YES unset   administratively down down

Enter the interface name that is facing the internet: serial0/0/1

Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
```

The final configuration for securing the IOS interface on the router R3 is also completed.

```
R3
Physical Config CLI Attributes
IOS Command Line Interface

Enter the security banner (Put the banner between
k and k, where k is any character):$Unauthorized access strictly prohibited!$
Enable secret is either not configured or
is the same as enable password
Enter the new enable secret: cisco
Confirm the enable secret: cisco
Enter the new enable password: cisco123
Confirm the enable password: cisco123

Configuration of local user database
Enter the username: admin
Enter the password: cisco
Confirm the password: cisco

Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: 10

Maximum Login failures with the device: 5

Maximum time period for crossing the failed login attempts: 5

Configure SSH server? [yes]: yes

Enter the host name: R3
Enter the domain-name: R3.domain
Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling CEF (This might impact the memory requirements for your platform)
Enabling unicast rpf on all interfaces connected
to internet

Configure CBAC Firewall feature? [yes/no]: yes

This is the configuration generated:
```

4.3.5. Control Plane Security

The last step is to apply control plan security on the router which will make sure routers are protected from all sort of insider attacks. In the screenshot attached below, it can be seen that router is not supporting all commands which means control plan security is enabled on the router.

```
R1
Physical Config CLI Attributes
IOS Command Line Interface

R1(config)#
R1(config)#
R1(config)#access-list 150 permit tcp any any
R1(config)#access-list 150 permit tcp any any eq 80
R1(config)#class-map secure-policy
R1(config-cmap)#match access-group 150
R1(config-cmap)#exit
R1(config)#policy-map secure-policy
^
% Invalid input detected at '^' marker.

R1(config)#policy-map secure-policy
R1(config-pmap)#class secure-policy
R1(config-pmap-c)#police rate 10000 pps
^
% Invalid input detected at '^' marker.

R1(config-pmap-c)#police ?
% Unrecognized command
R1(config-pmap-c)#police rate 10 pps
^
% Invalid input detected at '^' marker.

R1(config-pmap-c)#conform-action transmit
^
% Invalid input detected at '^' marker.

R1(config-pmap-c)#exit
R1(config-pmap)#exit
R1(config)#control-plane
^
% Invalid input detected at '^' marker.

R1(config)#
```

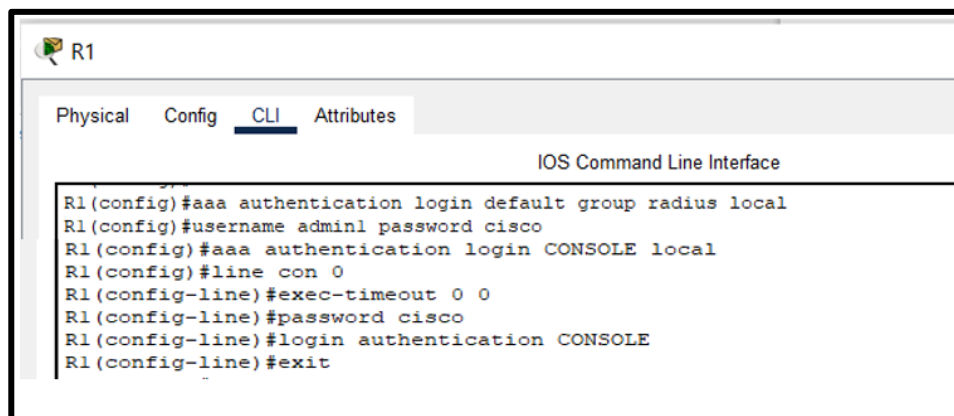
4.4. PART 3: AAA ON CISCO ROUTERS

4.4.1. AAA Explanation

AAA refers to Authentication, Authorization and Accounting, a type of security framework that allows the overall control to the resources of a network. Authentication is the process through which the user's identity who is attempting to access the network is being verified. The authentication process is typically done by entering the username and the password or by the biometric method. Accounting is the process of tracking and logging network user activities. This can involve tracking access attempts, resource use and other pertinent data. A network can enforce security measures that ensure only authorized users have access to network resources by adopting AAA. It also enables tracking and auditing of user activity, which can aid in the detection of security breaches or policy violations (Song, Wang and Song, 2008).

4.4.2. Implement AAA authentication

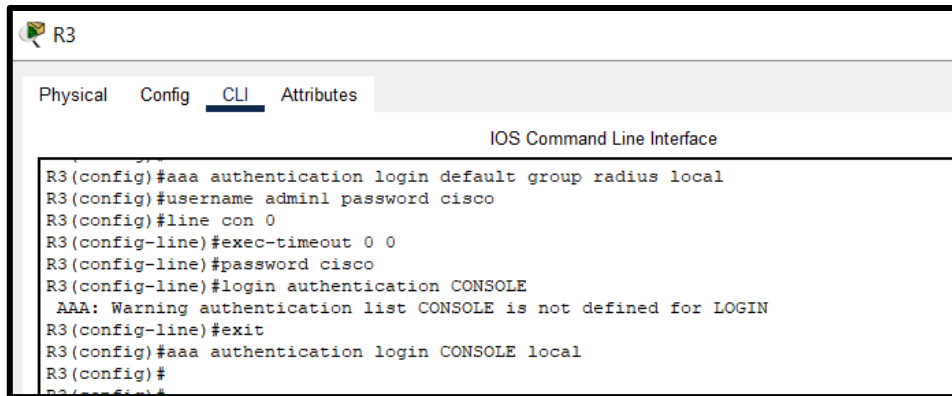
For the purpose of implementing AAA authentication on the network for local database, the router R1 is started where login default group is enabled. In addition to this, the login console local configuration is also done.

A screenshot of the Cisco IOS Command Line Interface (CLI) for router R1. The interface shows the configuration mode with the following commands entered:

```
R1(config)#aaa authentication login default group radius local
R1(config)#username admin1 password cisco
R1(config)#aaa authentication login CONSOLE local
R1(config)#line con 0
R1(config-line)#exec-timeout 0 0
R1(config-line)#password cisco
R1(config-line)#login authentication CONSOLE
R1(config-line)#exit
```

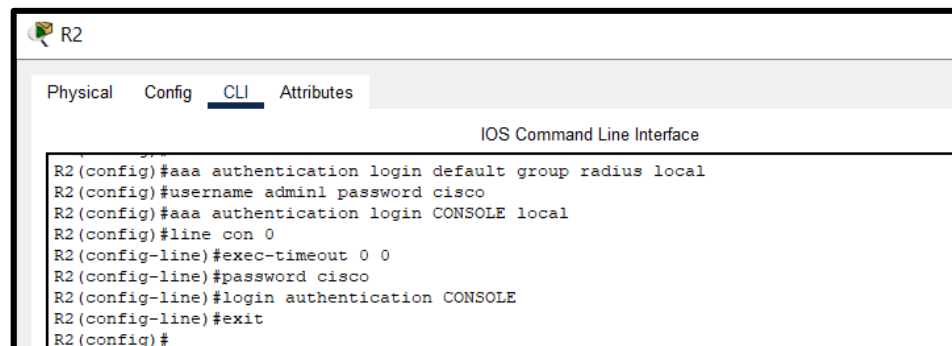
The CLI window has tabs for Physical, Config, CLI (selected), and Attributes. The title bar indicates it is the IOS Command Line Interface for R1.

In the case of router R3, the AAA authentication login group radius local is performed and password is set as Cisco (Song, Wang and Song, 2008).

A screenshot of the Cisco Packet Tracer interface for router R3. The 'CLI' tab is selected under the 'Config' menu. The terminal window shows the following commands and output:

```
R3(config)#aaa authentication login default group radius local
R3(config)#username admin1 password cisco
R3(config)#line con 0
R3(config-line)#exec-timeout 0 0
R3(config-line)#password cisco
R3(config-line)#login authentication CONSOLE
AAA: Warning authentication list CONSOLE is not defined for LOGIN
R3(config-line)#exit
R3(config)#aaa authentication login CONSOLE local
R3(config)#
```

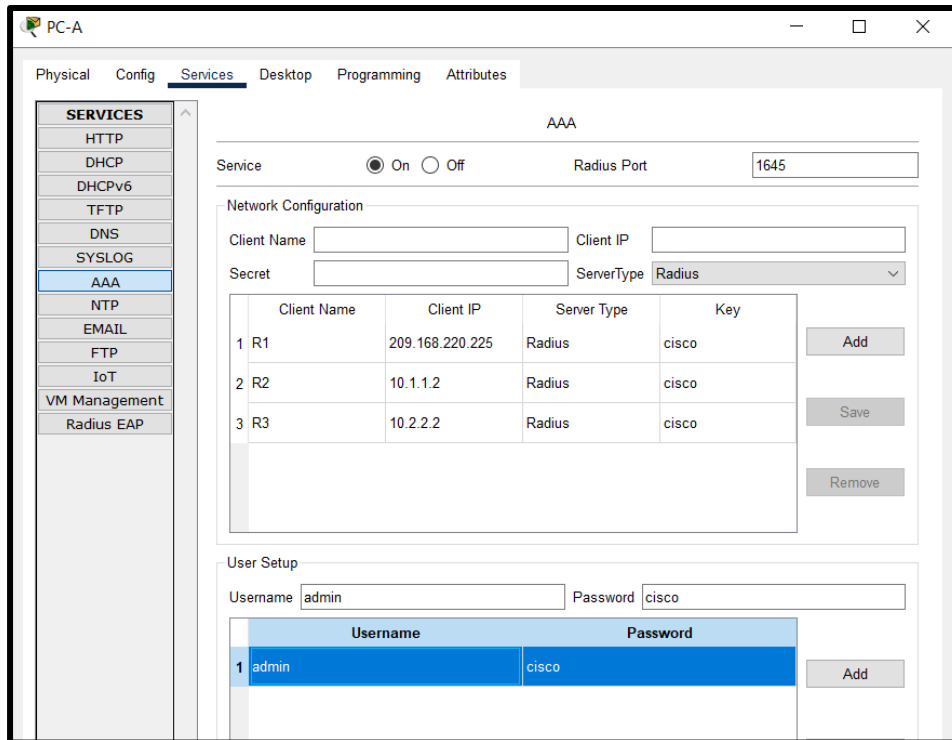
In the case of router R2, the same authentication is performed with password set up on the router.

A screenshot of the Cisco Packet Tracer interface for router R2. The 'CLI' tab is selected under the 'Config' menu. The terminal window shows the following commands and output:

```
R2(config)#aaa authentication login default group radius local
R2(config)#username admin1 password cisco
R2(config)#aaa authentication login CONSOLE local
R2(config)#line con 0
R2(config-line)#exec-timeout 0 0
R2(config-line)#password cisco
R2(config-line)#login authentication CONSOLE
R2(config-line)#exit
R2(config)#
```

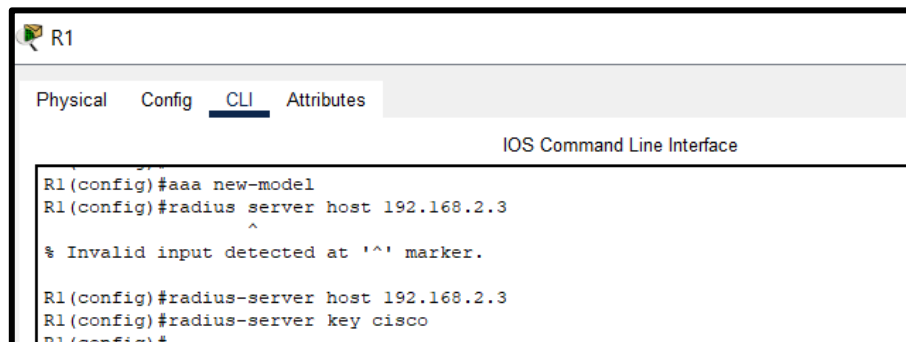
4.4.3. Cisco Secure ACS

Herein, the configuration for the Cisco secure ACS is performed by selecting services and selecting AAA. Under AAA service, the service is turned on, radius port is assigned with 1645 and clients are added with their IP address, secret and client name.

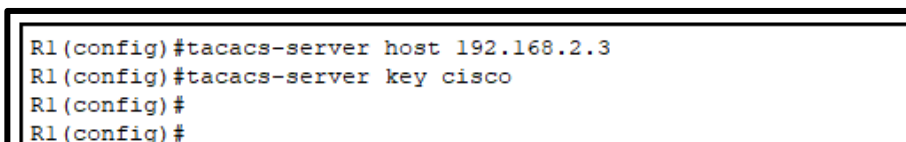


4.4.4. Server-based AAA Authentication

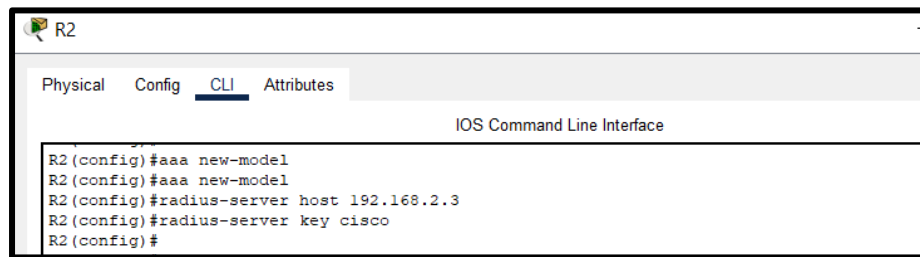
When it comes to server based AAA authentication, there will be a need for setting up a new model on the routers. In the screenshot attached below, radius server IP address, host IP address and key are assigned.



The TACACS+ server host IP address and a key has also been assigned.

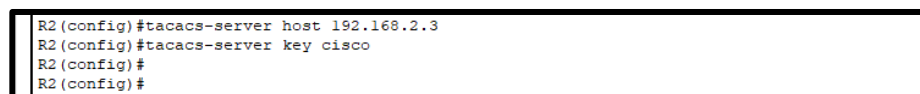


When it comes to the router R2, the AAA new model is created and host IP address and key has been assigned.

A screenshot of the Cisco Packet Tracer interface for router R2. The 'CLI' tab is selected under the 'Config' menu. The command prompt shows the following configuration steps: creating a new AAA model, assigning a host IP of 192.168.2.3, and setting a key of 'cisco'.

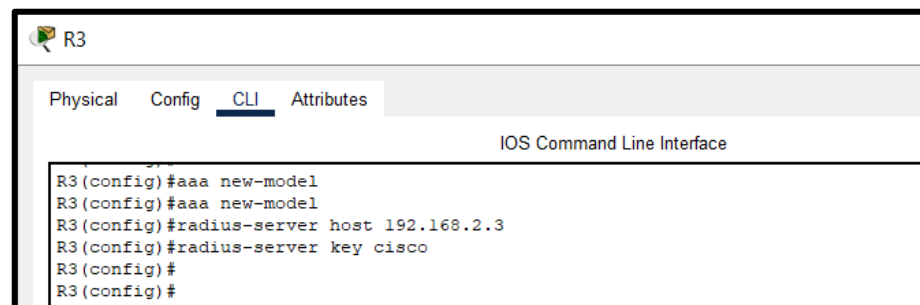
```
R2
R2(config)#aaa new-model
R2(config)#aaa new-model
R2(config)#radius-server host 192.168.2.3
R2(config)#radius-server key cisco
R2(config)#
```

For the TACACS+ server also, the host IP address is assigned along with a key.

A screenshot of the Cisco Packet Tracer interface for router R2, showing the configuration for a TACACS+ server. The commands show the assignment of a host IP address and a key to the TACACS+ server.

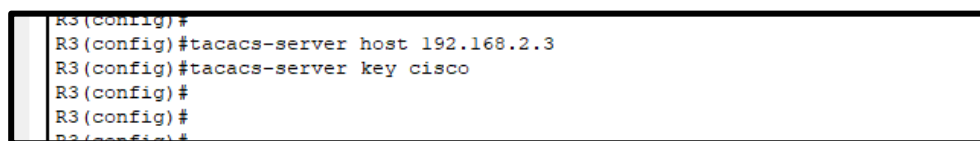
```
R2(config)#tacacs-server host 192.168.2.3
R2(config)#tacacs-server key cisco
R2(config)#
R2(config)#
```

In the case of router R3 also, the AAA new model is created and this model host is assigned with IP address and a key.

A screenshot of the Cisco Packet Tracer interface for router R3. The 'CLI' tab is selected under the 'Config' menu. The command prompt shows the following configuration steps: creating a new AAA model, assigning a host IP of 192.168.2.3, and setting a key of 'cisco'.

```
R3
R3(config)#aaa new-model
R3(config)#aaa new-model
R3(config)#radius-server host 192.168.2.3
R3(config)#radius-server key cisco
R3(config)#
R3(config)#
```

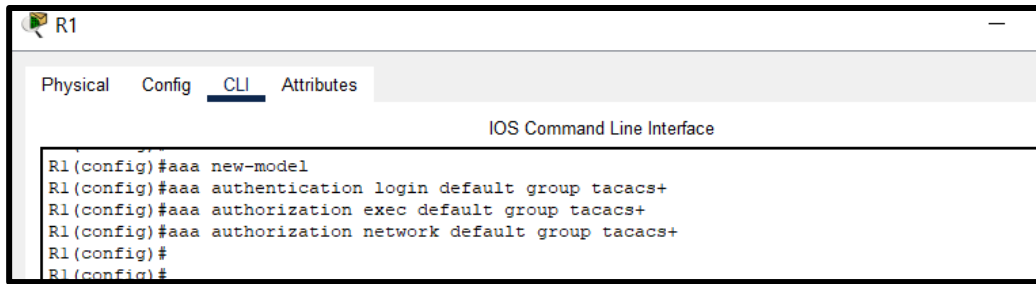
Finally, for the TACACS+ server, the host IP address and key is also assigned.

A screenshot of the Cisco Packet Tracer interface for router R3, showing the configuration for a TACACS+ server. The commands show the assignment of a host IP address and a key to the TACACS+ server.

```
R3(config)#
R3(config)#tacacs-server host 192.168.2.3
R3(config)#tacacs-server key cisco
R3(config)#
R3(config)#
R3(config)#
```

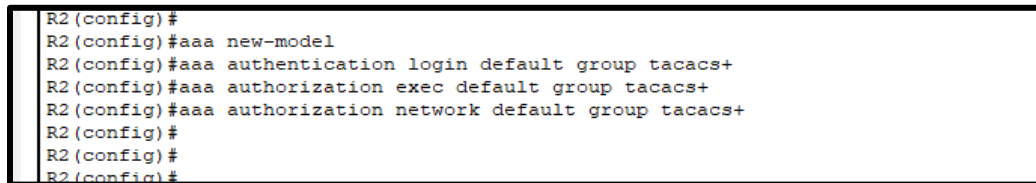
4.4.5. Server-based AAA Authorization and Accounting

For the purpose of setting up server based AAA authorization and accounting, the router R1 configuration is done where a new login default, exec default and network default groups are created.

A screenshot of a network simulator window titled 'R1'. It has tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' selected. The window shows the 'IOS Command Line Interface' with the following commands entered:

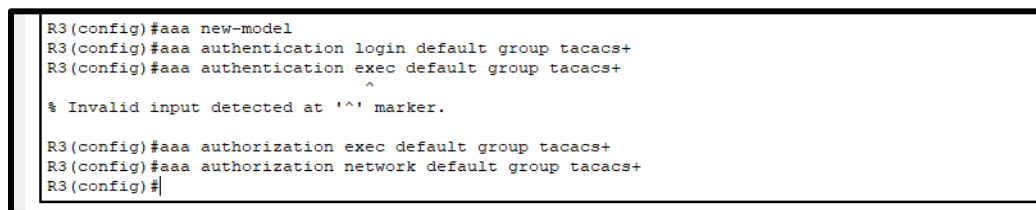
```
R1(config)#aaa new-model
R1(config)#aaa authentication login default group tacacs+
R1(config)#aaa authorization exec default group tacacs+
R1(config)#aaa authorization network default group tacacs+
R1(config)#
R1(config)#
```

In the case of router R2 also, the login, exec and network default groups are being created using TACACS+.

A screenshot of a network simulator window titled 'R2'. It shows the 'IOS Command Line Interface' with the following commands entered:

```
R2(config)#
R2(config)#aaa new-model
R2(config)#aaa authentication login default group tacacs+
R2(config)#aaa authorization exec default group tacacs+
R2(config)#aaa authorization network default group tacacs+
R2(config)#
R2(config)#
R2(config)#
```

Finally, for the router R3 also, the login, exec and network default groups are created for the TACACS+ server.

A screenshot of a network simulator window titled 'R3'. It shows the 'IOS Command Line Interface' with the following commands entered:

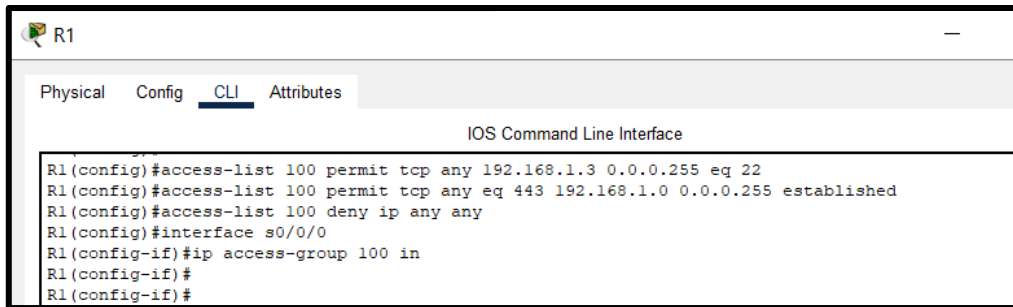
```
R3(config)#aaa new-model
R3(config)#aaa authentication login default group tacacs+
R3(config)#aaa authentication exec default group tacacs+
^
% Invalid input detected at '^' marker.

R3(config)#aaa authorization exec default group tacacs+
R3(config)#aaa authorization network default group tacacs+
R3(config)#
```

4.5. PART 4: MITIGATE THREATS USING ACLS

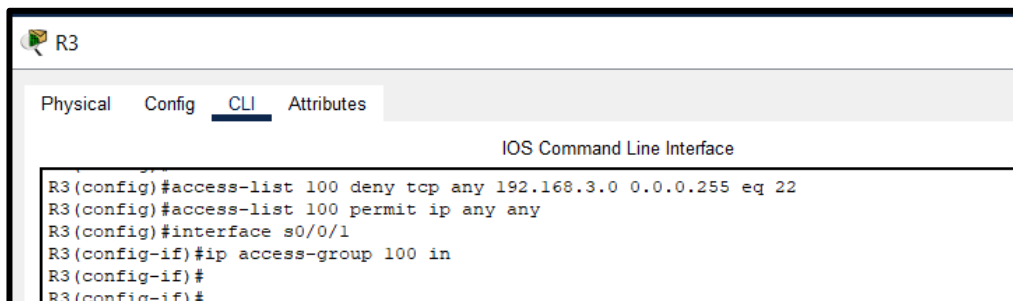
4.5.1. Implement ACLs

When it comes to filtering traffic and mitigating all types of network attacks, it can be said that there is a need for access control list on a network. On the router R1, ACL has been applied that will allow/deny particular IP address from accessing the network. After applying ACL rule, the interface is also assigned and access group command is executed (Song, Wang and Song, 2008).

A screenshot of the Cisco Packet Tracer interface for router R1. The 'CLI' tab is selected under the 'Config' menu. The command prompt shows the following configuration steps: creating an extended ACL 100 to permit TCP traffic from 192.168.1.3 to 192.168.1.0 on port 22, denying all other IP traffic, and applying this ACL to the s0/0/0 interface in the inbound direction.

```
R1
R1(config)#access-list 100 permit tcp any 192.168.1.3 0.0.0.255 eq 22
R1(config)#access-list 100 permit tcp any eq 443 192.168.1.0 0.0.0.255 established
R1(config)#access-list 100 deny ip any any
R1(config)#interface s0/0/0
R1(config-if)#ip access-group 100 in
R1(config-if)#
```

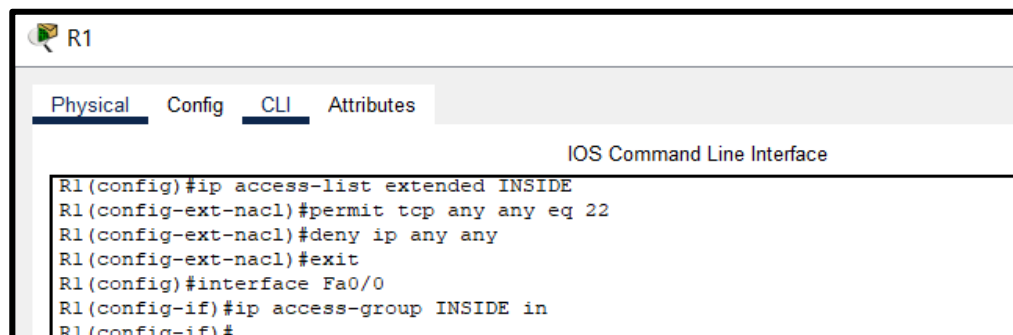
The implementation for the ACL is also applied on the router R2 and R3 following same configurations as router R1 (Chow et al., 2005).

A screenshot of the Cisco Packet Tracer interface for router R3. The 'CLI' tab is selected under the 'Config' menu. The command prompt shows the following configuration steps: creating an extended ACL 100 to deny TCP traffic from 192.168.3.0 to 192.168.3.0 on port 22, permitting all other IP traffic, and applying this ACL to the s0/0/1 interface in the inbound direction.

```
R3
R3(config)#access-list 100 deny tcp any 192.168.3.0 0.0.0.255 eq 22
R3(config)#access-list 100 permit ip any any
R3(config)#interface s0/0/1
R3(config-if)#ip access-group 100 in
R3(config-if)#
```

4.5.2. Classic Firewall Configuration

In the next proceeding step, the classic firewall configuration is started where extended ACL List is applied to the inside. This has been done by permitting IP address and selecting out router interface.

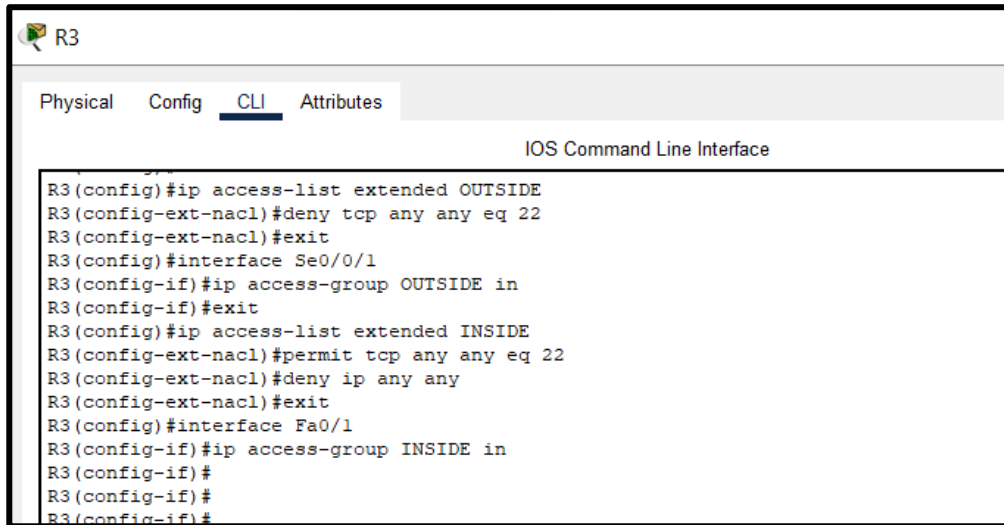
A screenshot of the Cisco Packet Tracer interface for router R1. The 'CLI' tab is selected under the 'Config' menu. The command prompt shows the following configuration steps: creating an extended named ACL 'INSIDE' to permit all TCP traffic and deny all other IP traffic, and applying this ACL to the Fa0/0 interface in the outbound direction.

```
R1
R1(config)#ip access-list extended INSIDE
R1(config-ext-nacl)#permit tcp any any eq 22
R1(config-ext-nacl)#deny ip any any
R1(config-ext-nacl)#exit
R1(config)#interface Fa0/0
R1(config-if)#ip access-group INSIDE out
R1(config-if)#
```

Along with inside rule, the outside rule is also applied and router interface is also assigned.

```
R1(config-if)#exit
R1(config)#ip access-list extended OUTSIDE
R1(config-ext-nacl)#deny tcp any any eq 22
R1(config-ext-nacl)#exit
R1(config)#interface se0/0/0
R1(config-if)#ip access-group OUTSIDE in
R1(config-if)#
```

The same configuration is followed for the router R3 and the same configuration is provided in the screenshot below.



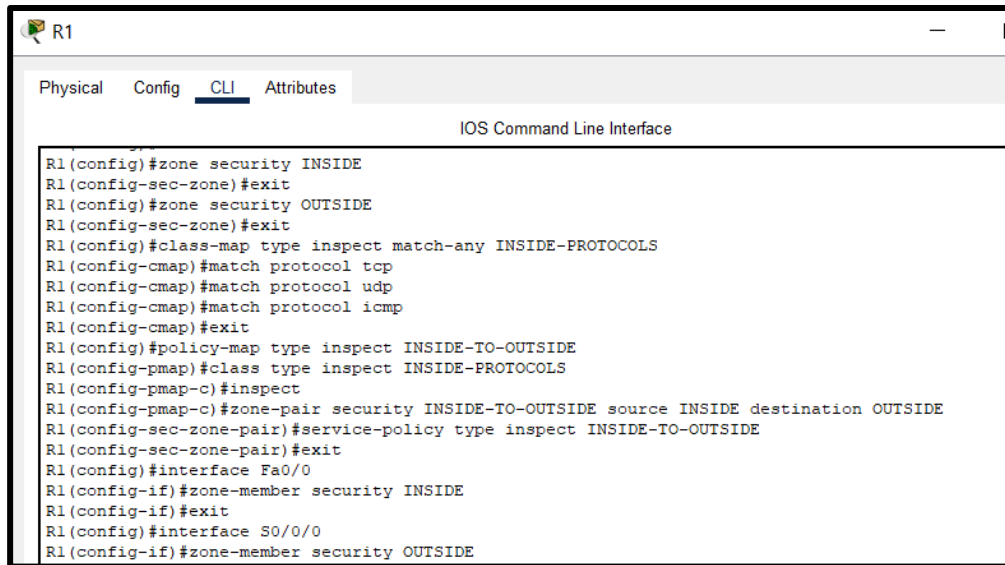
The screenshot shows the CLI of router R3 with the following configuration commands entered:

```
R3
Physical Config CLI Attributes
IOS Command Line Interface

R3(config)#ip access-list extended OUTSIDE
R3(config-ext-nacl)#deny tcp any any eq 22
R3(config-ext-nacl)#exit
R3(config)#interface Se0/0/1
R3(config-if)#ip access-group OUTSIDE in
R3(config-if)#exit
R3(config)#ip access-list extended INSIDE
R3(config-ext-nacl)#permit tcp any any eq 22
R3(config-ext-nacl)#deny ip any any
R3(config-ext-nacl)#exit
R3(config)#interface Fa0/1
R3(config-if)#ip access-group INSIDE in
R3(config-if)#
R3(config-if)#
R3(config-if)#
```

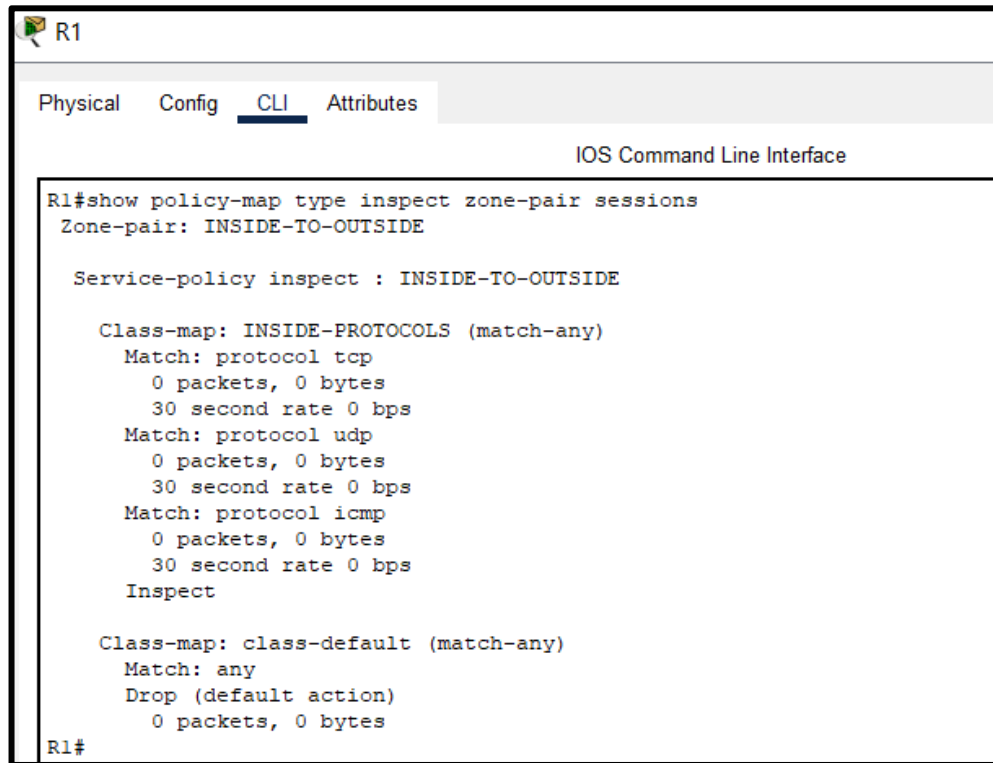
4.5.3. Zone-Based Policy Firewall

For the purpose of setting up zone based firewall, the zone security inside and outside commands are executed and relevant protocols are assigned i.e. TCP, UDP and ICMP. Along with protocols, other settings were also configured as shown in the screenshot attached below (Chow et al., 2005).

A screenshot of a network router's CLI interface. The window title is 'R1'. At the top, there are tabs for 'Physical', 'Config', 'CLI' (which is selected), and 'Attributes'. Below the tabs, the text 'IOS Command Line Interface' is displayed. The main area shows a series of configuration commands entered in a single line, with the prompt 'R1(config)#' at the beginning of each line. The commands configure a zone-based firewall by defining inside and outside security zones, creating a class-map for inspecting TCP, UDP, and ICMP traffic, defining a policy-map to inspect traffic from inside to outside, and applying these configurations to interfaces Fa0/0 and S0/0/0.

```
R1(config)#zone security INSIDE
R1(config-sec-zone)#exit
R1(config)#zone security OUTSIDE
R1(config-sec-zone)#exit
R1(config)#class-map type inspect match-any INSIDE-PROTOCOLS
R1(config-cmap)#match protocol tcp
R1(config-cmap)#match protocol udp
R1(config-cmap)#match protocol icmp
R1(config-cmap)#exit
R1(config)#policy-map type inspect INSIDE-TO-OUTSIDE
R1(config-pmap)#class type inspect INSIDE-PROTOCOLS
R1(config-pmap-c)#inspect
R1(config-pmap-c)#zone-pair security INSIDE-TO-OUTSIDE source INSIDE destination OUTSIDE
R1(config-sec-zone-pair)#service-policy type inspect INSIDE-TO-OUTSIDE
R1(config-sec-zone-pair)#exit
R1(config)#interface Fa0/0
R1(config-if)#zone-member security INSIDE
R1(config-if)#exit
R1(config)#interface S0/0/0
R1(config-if)#zone-member security OUTSIDE
```

As the configuration for the zone based firewall has been done, the use of show command is done to list out all configurations.

A screenshot of the same network router's CLI interface. The window title is 'R1'. The tabs 'Physical', 'Config', 'CLI' (selected), and 'Attributes' are visible. Below the tabs, the text 'IOS Command Line Interface' is displayed. The main area shows the output of the command 'show policy-map type inspect zone-pair sessions'. The output displays the configuration for the 'INSIDE-TO-OUTSIDE' zone-pair, including the service-policy 'inspect', the class-map 'INSIDE-PROTOCOLS' with matches for TCP, UDP, and ICMP, and the class-map 'class-default' with a default drop action.

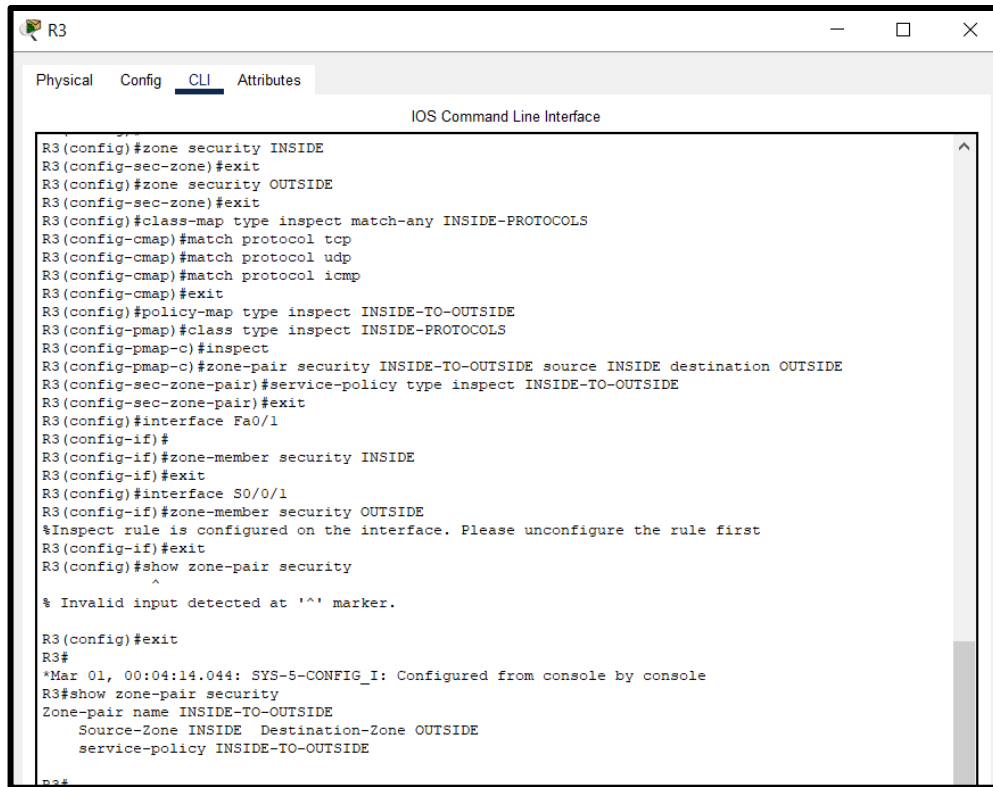
```
R1#show policy-map type inspect zone-pair sessions
Zone-pair: INSIDE-TO-OUTSIDE

Service-policy inspect : INSIDE-TO-OUTSIDE

Class-map: INSIDE-PROTOCOLS (match-any)
  Match: protocol tcp
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol udp
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol icmp
    0 packets, 0 bytes
    30 second rate 0 bps
  Inspect

Class-map: class-default (match-any)
  Match: any
  Drop (default action)
    0 packets, 0 bytes
R1#
```

The zone based firewall configuration is done on the router R2 and R3 which has been shown in the below attached screenshot.



```
R3
Physical Config CLI Attributes
IOS Command Line Interface
R3(config)#zone security INSIDE
R3(config-sec-zone)#exit
R3(config)#zone security OUTSIDE
R3(config-sec-zone)#exit
R3(config)#class-map type inspect match-any INSIDE-PROTOCOLS
R3(config-cmap)#match protocol tcp
R3(config-cmap)#match protocol udp
R3(config-cmap)#match protocol icmp
R3(config-cmap)#exit
R3(config)#policy-map type inspect INSIDE-TO-OUTSIDE
R3(config-pmap)#class type inspect INSIDE-PROTOCOLS
R3(config-pmap-c)#inspect
R3(config-pmap-c)#zone-pair security INSIDE-TO-OUTSIDE source INSIDE destination OUTSIDE
R3(config-sec-zone-pair)#service-policy type inspect INSIDE-TO-OUTSIDE
R3(config-sec-zone-pair)#exit
R3(config)#interface Fa0/1
R3(config-if)#
R3(config-if)#zone-member security INSIDE
R3(config-if)#exit
R3(config)#interface S0/0/1
R3(config-if)#zone-member security OUTSIDE
%Inspect rule is configured on the interface. Please unconfigure the rule first
R3(config-if)#exit
R3(config)#show zone-pair security
^
% Invalid input detected at '^' marker.

R3(config)#exit
R3#
*Mar 01, 00:04:14.044: SYS-5-CONFIG_I: Configured from console by console
R3#show zone-pair security
Zone-pair name INSIDE-TO-OUTSIDE
Source-Zone INSIDE Destination-Zone OUTSIDE
service-policy INSIDE-TO-OUTSIDE
R3#
```

4.6. PART 5: IMPLEMENT SECURE NETWORK DESIGN, MANAGEMENT AND REPORTING

4.6.1. Implementation of a Comprehensive Security Policy

A comprehensive security policy is a set of standards and processes meant to keep a network secure. All areas of network security, including access control, data protection and incident response, should be covered by the policy. The first stage in developing a comprehensive security strategy is to define the network's specific security requirements. This includes identifying the types of data held on the network, potential network risks and regulatory criteria that the network must meet. Once the security requirements have been defined, a policy should be developed to meet those requirements. Guidelines for access control, data protection, network monitoring, incident response and employee training should all be included in the policy. Access control policies should specify who has access to

the network and its resources. Password restrictions, multi-factor authentication requirements and physical security measures like access control systems are examples of such measures (Chow et al., 2005).

4.6.2. Techniques and tools for Network Security Testing

Network security testing is the process through which the overall security of the network is evaluated. The network security testing is done so that the network can detect the vulnerabilities and the threats to the network. The tools which are used in the vulnerability scanning are Threat spy, API Sec, App Scan, etc. The second one is penetration testing, this technique stimulates an attack on the network so that if there is any vulnerability it may be detected and removed. Another technique is network mapping, in case to identify all the devices that are connected to the network this tool maps the network so that it can identify the points from where the attacker can attack the network. Tools that are used in the network mapping are the Microsoft Visio, Solar Winds Network Topology Mapper, etc. Lastly, there is network monitoring, this technique refers to monitoring the network by the help of tools like intrusion detection systems, honey pot systems and so on (Agar, Grgić and Rimac-Drlje, 2007).

4.7. PART 6: MITIGATE COMMON LAYER 2 ATTACKS

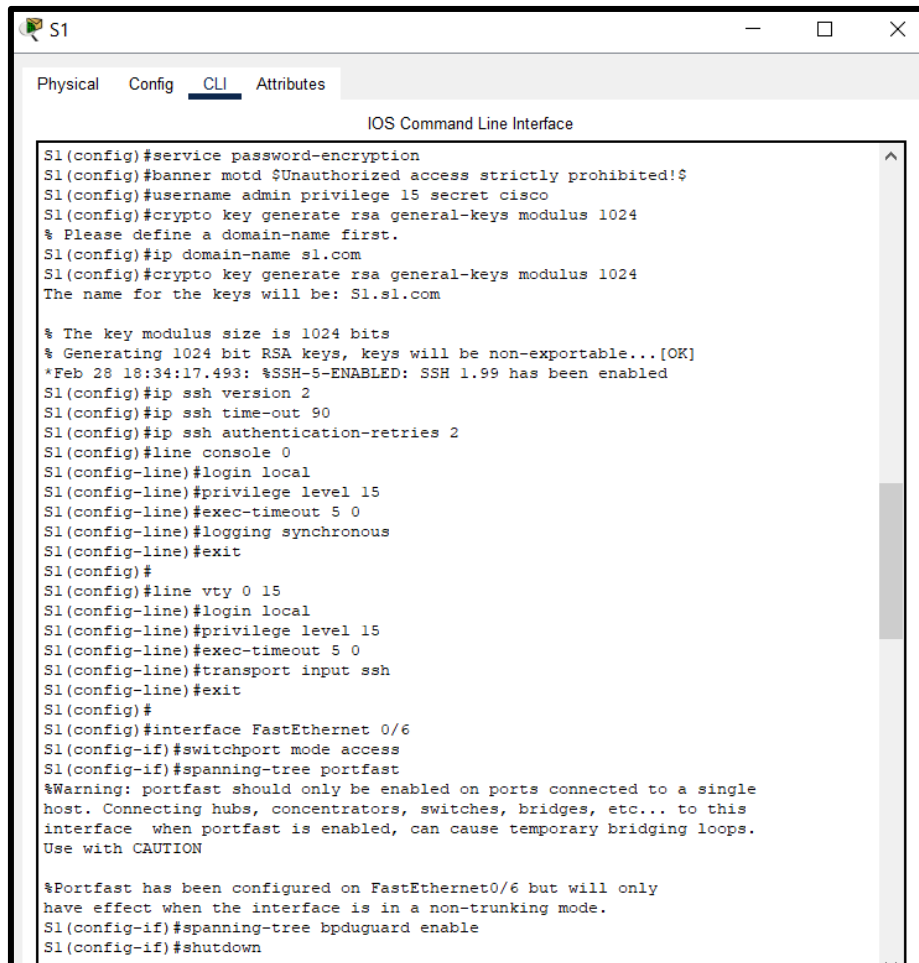
4.7.1. Vulnerabilities and Mitigation techniques

Layer 2 infrastructure is in charge of data packet routing within a local area network (LAN). Switches and bridges connect network devices including PCs, printers and servers. Layer 2 infrastructure vulnerabilities include the vulnerabilities like MAC address spoofing, spanning tree protocol attack, VLAN hopping and ARP spoofing. In MAC address spoofing the attackers can initiate another device by spoofing its mac address. Techniques that are used for mitigating this vulnerability include port security and MAC address filtering. The next

vulnerability is the spanning tree protocol attacks, in this the attacker can leverage the STP flaws to disrupt the networks or can reroute the traffic to a rogue device. In VLAN hopping, the attackers gain access to the sensitive data or start attacks on other VLANs by exploiting the VLAN configuration mistakes. Implementing the VLAN access control lists (ACLs) and employing Private VLANs are the two mitigation approaches for this vulnerability.

4.7.2. Switch Security

For the purpose of switch security to mitigate LAN based attacks, there is a major need for configuring a network switch. In the screenshot attached below, the service password encryption is enabled, administrator privileges are set, password is set and other configurations.

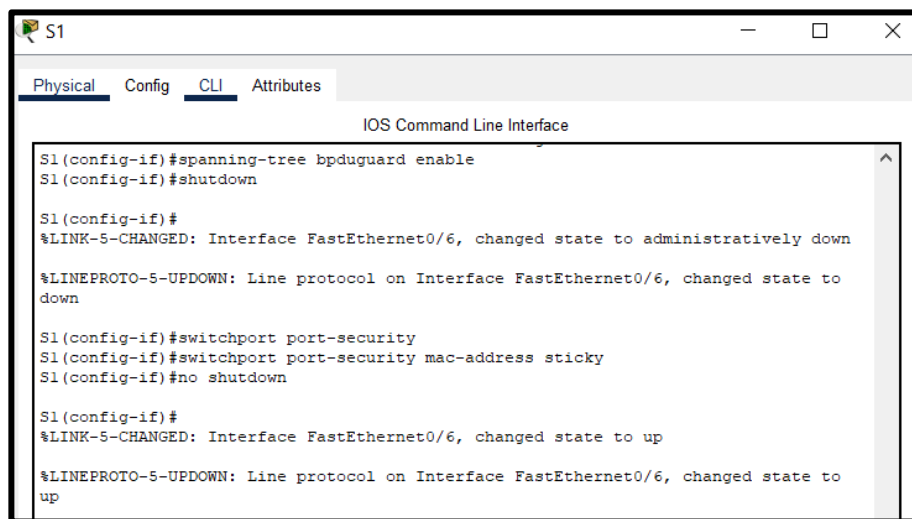


```
S1(config)#service password-encryption
S1(config)#banner motd $Unauthorized access strictly prohibited!$
S1(config)#username admin privilege 15 secret cisco
S1(config)#crypto key generate rsa general-keys modulus 1024
% Please define a domain-name first.
S1(config)#ip domain-name sl.com
S1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: S1.sl.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Feb 28 18:34:17.493: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#ip ssh version 2
S1(config)#ip ssh time-out 90
S1(config)#ip ssh authentication-retries 2
S1(config)#line console 0
S1(config-line)#login local
S1(config-line)#privilege level 15
S1(config-line)#exec-timeout 5 0
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#privilege level 15
S1(config-line)#exec-timeout 5 0
S1(config-line)#transport input ssh
S1(config-line)#exit
S1(config)#
S1(config)#interface FastEthernet 0/6
S1(config-if)#switchport mode access
S1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/6 but will only
have effect when the interface is in a non-trunking mode.
S1(config-if)#spanning-tree bpduguard enable
S1(config-if)#shutdown
```

For the switch S1, the STP guard is enabled along with port security and interface state is changed to up state.



```
S1
Physical Config CLI Attributes
IOS Command Line Interface

S1(config-if)#spanning-tree bpduguard enable
S1(config-if)#shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

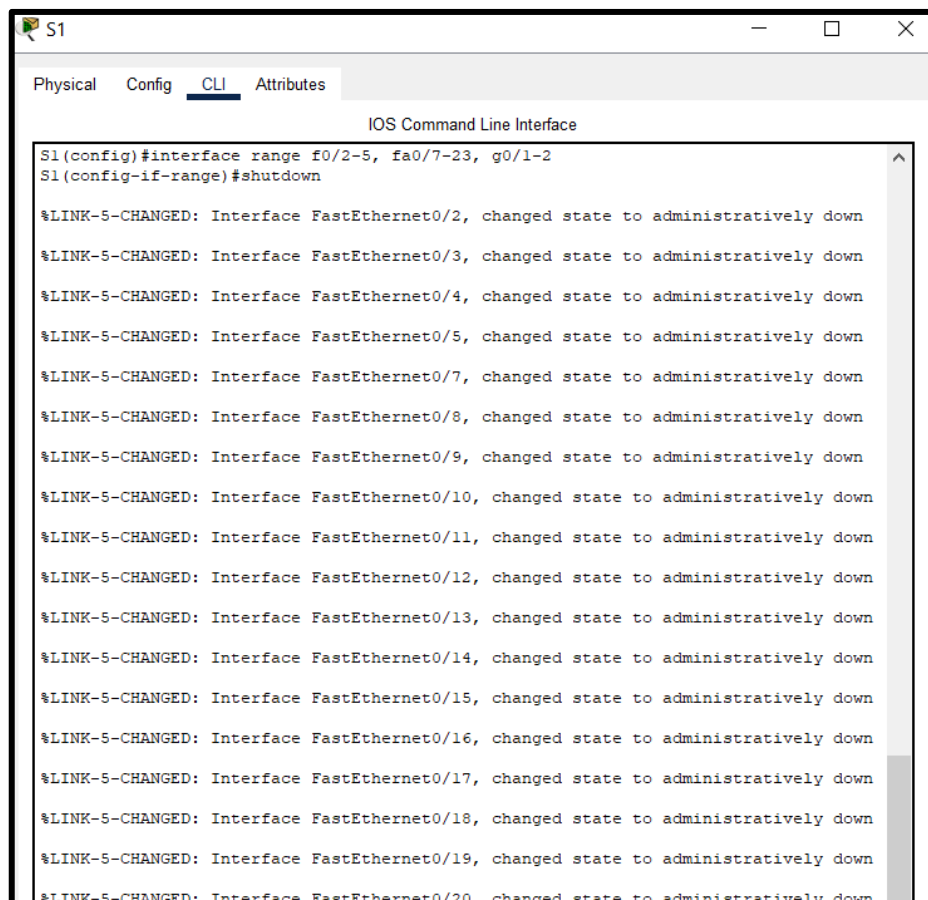
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to down

S1(config-if)#switchport port-security
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up
```

Shutting down un-used ports by executing ‘shutdown’ command (Liu, Barber and DiGrande, 2009).

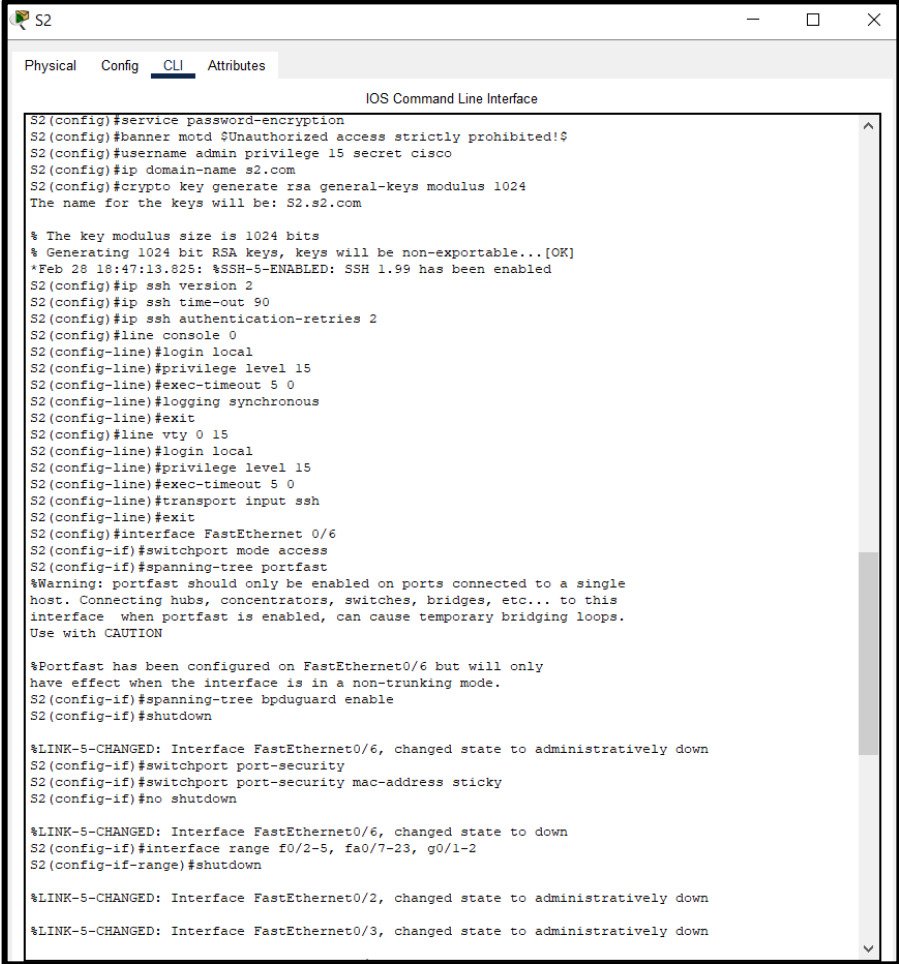


```
S1
Physical Config CLI Attributes
IOS Command Line Interface

S1(config)#interface range f0/2-5, fa0/7-23, g0/1-2
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
```

The same configuration is followed for the switch S2 in order to protect network switches from LAN based attacks.



```
S2
Physical Config CLI Attributes
IOS Command Line Interface

S2(config)#service password-encryption
S2(config)#banner motd $Unauthorized access strictly prohibited!$
S2(config)#username admin privilege 15 secret cisco
S2(config)#ip domain-name s2.com
S2(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: S2.s2.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Feb 28 18:47:13.825: %SSH-5-ENABLED: SSH 1.99 has been enabled
S2(config)#ip ssh version 2
S2(config)#ip ssh time-out 90
S2(config)#ip ssh authentication-retries 2
S2(config)#line console 0
S2(config-line)#login local
S2(config-line)#privilege level 15
S2(config-line)#exec-timeout 5 0
S2(config-line)#logging synchronous
S2(config-line)#exit
S2(config)#line vty 0 15
S2(config-line)#login local
S2(config-line)#privilege level 15
S2(config-line)#exec-timeout 5 0
S2(config-line)#transport input ssh
S2(config-line)#exit
S2(config)#interface FastEthernet 0/6
S2(config-if)#switchport mode access
S2(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

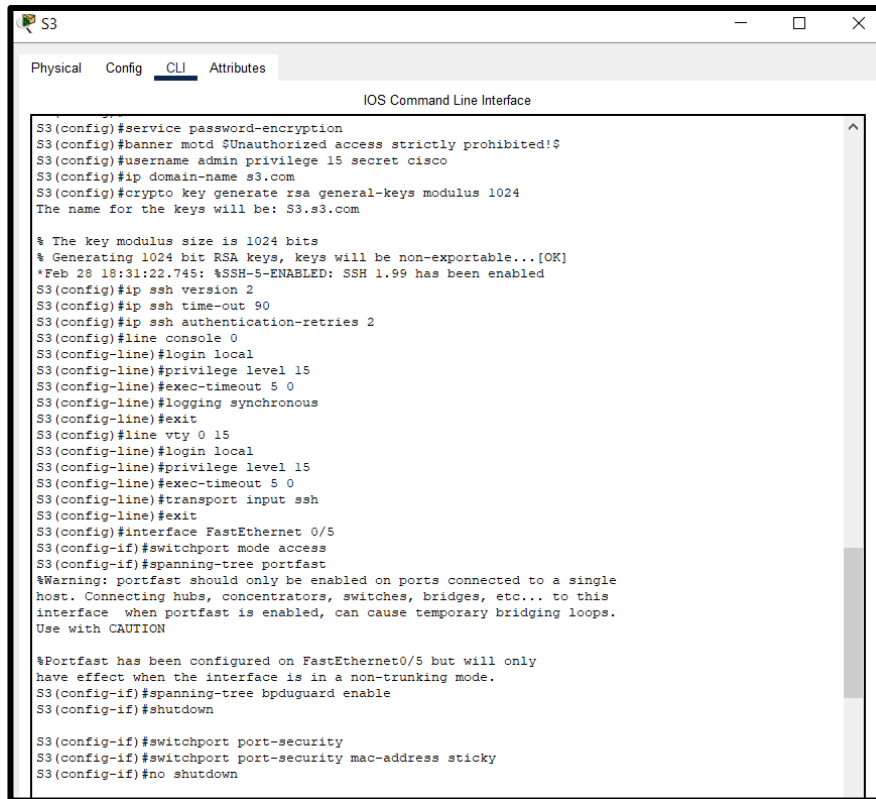
%Portfast has been configured on FastEthernet0/6 but will only
have effect when the interface is in a non-trunking mode.
S2(config-if)#spanning-tree bpduguard enable
S2(config-if)#shutdown

%LINK-S-CHANGED: Interface FastEthernet0/6, changed state to administratively down
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#no shutdown

%LINK-S-CHANGED: Interface FastEthernet0/6, changed state to down
S2(config-if)#interface range f0/2-5, fa0/7-23, g0/1-2
S2(config-if-range)#shutdown

%LINK-S-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINK-S-CHANGED: Interface FastEthernet0/3, changed state to administratively down
```

Similarly, in the case of switch S3 also, the same configuration is performed to protect the switch from possible LAN based attacks.

A screenshot of a Cisco IOS Command Line Interface window titled 'S3'. The window has tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' selected. The CLI shows a configuration session for S3. The user enters 'service password-encryption', then 'banner motd \$Unauthorized access strictly prohibited!\$'. Next, they set 'username admin privilege 15 secret cisco' and 'ip domain-name s3.com'. Then, they generate RSA keys with 'crypto key generate rsa general-keys modulus 1024'. The system outputs information about the key generation, including the modulus size and the SSH version. The user then configures SSH with 'ssh version 2', 'ssh time-out 90', and 'ssh authentication-retries 2'. They also configure the console and vty lines with 'login local', 'privilege level 15', and 'exec-timeout 5 0'. Finally, they configure the FastEthernet 0/5 interface as a switchport in access mode, enable portfast, and configure port-security with 'mac-address sticky' and 'no shutdown'.

```
S3(config)#service password-encryption
S3(config)#banner motd $Unauthorized access strictly prohibited!$
S3(config)#username admin privilege 15 secret cisco
S3(config)#ip domain-name s3.com
S3(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: S3.s3.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Feb 28 18:31:22.745: %SSH-5-ENABLED: SSH 1.99 has been enabled
S3(config)#ip ssh version 2
S3(config)#ip ssh time-out 90
S3(config)#ip ssh authentication-retries 2
S3(config)#line console 0
S3(config-line)#login local
S3(config-line)#privilege level 15
S3(config-line)#exec-timeout 5 0
S3(config-line)#logging synchronous
S3(config-line)#exit
S3(config)#line vty 0 15
S3(config-line)#login local
S3(config-line)#privilege level 15
S3(config-line)#exec-timeout 5 0
S3(config-line)#transport input ssh
S3(config-line)#exit
S3(config)#interface FastEthernet 0/5
S3(config-if)#switchport mode access
S3(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

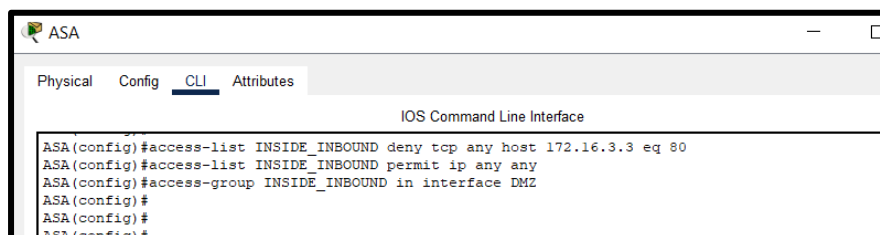
%Portfast has been configured on FastEthernet0/5 but will only
have effect when the interface is in a non-trunking mode.
S3(config-if)#spanning-tree bpduguard enable
S3(config-if)#shutdown

S3(config-if)#switchport port-security
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#no shutdown
```

4.8. PART 7: IMPLEMENT THE CISCO IOS FIREWALL

4.8.1. Implement ACLs

When it comes to the implementation of the access control lists on the ASA firewall, it can be said that there is a need for permitting and denying inside sets. The screenshot attached below shows the execution of inside inbound commands that denies a particular TCP host on the network.

A screenshot of a Cisco ASA Command Line Interface window titled 'ASA'. The window has tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' selected. The CLI shows a configuration session for ASA. The user enters 'access-list INSIDE_INBOUND deny tcp any host 172.16.3.3 eq 80', then 'access-list INSIDE_INBOUND permit ip any any', and finally 'access-group INSIDE_INBOUND in interface DMZ'.

```
ASA(config)#access-list INSIDE_INBOUND deny tcp any host 172.16.3.3 eq 80
ASA(config)#access-list INSIDE_INBOUND permit ip any any
ASA(config)#access-group INSIDE_INBOUND in interface DMZ
ASA(config)#
```

4.8.2. Classic Firewall

The use of Cisco Packet tracer has been done to configure the classic firewall but it is not supported by the simulation software.

4.8.3. Zone-Based Policy Firewall

The use of Cisco Packet tracer has been done to configure the classic firewall but it is not supported by the simulation software.

4.9. PART 8: IMPLEMENT THE CISCO IOS IPS FEATURE SET

4.9.1. Network-based Intrusion Prevention Systems

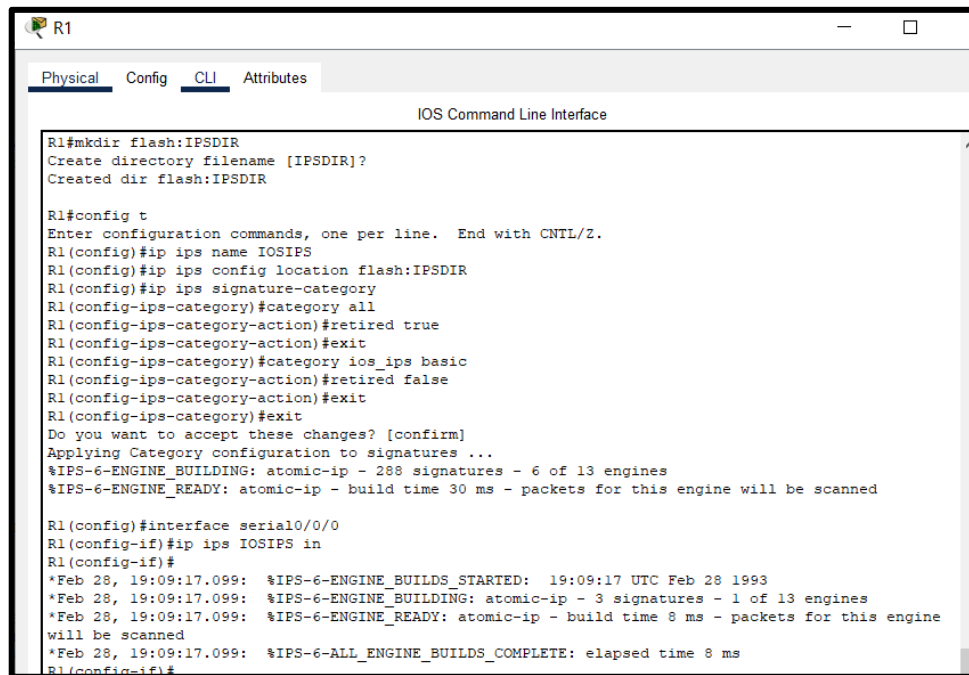
Intrusion Prevention Systems (IPS) are network-based systems that identify and prevent hostile network traffic. These systems are strategically placed throughout the network to monitor traffic and enforce security standards. To detect and stop threats, they employ signature-based detection, anomaly detection and behavior-based analysis. To improve network speed, IPS can also do packet filtering and traffic shaping (Liu, Barber and DiGrande, 2009).

4.9.2. Signatures Use

Signatures are types of pattern recognition that intrusion detection and prevention systems use to identify known threats. A signature is a distinct string of data that corresponds to a specific type of malware or assault. The signature may contain network protocols, port numbers, payload content and other attack-related information. Signatures can be made manually or automatically through the use of machine learning methods. Signatures are used for the speedy detection of recognized threats and it also reduces false positives by concentrating on certain attack characteristics.

4.9.3. Configure Cisco IOS IPS operations

Now, the intrusion prevention system configuration is also started on the router R1. It usually starts from IPS name configuration, basic rule configuration, and other several settings as shown in the screenshot below.



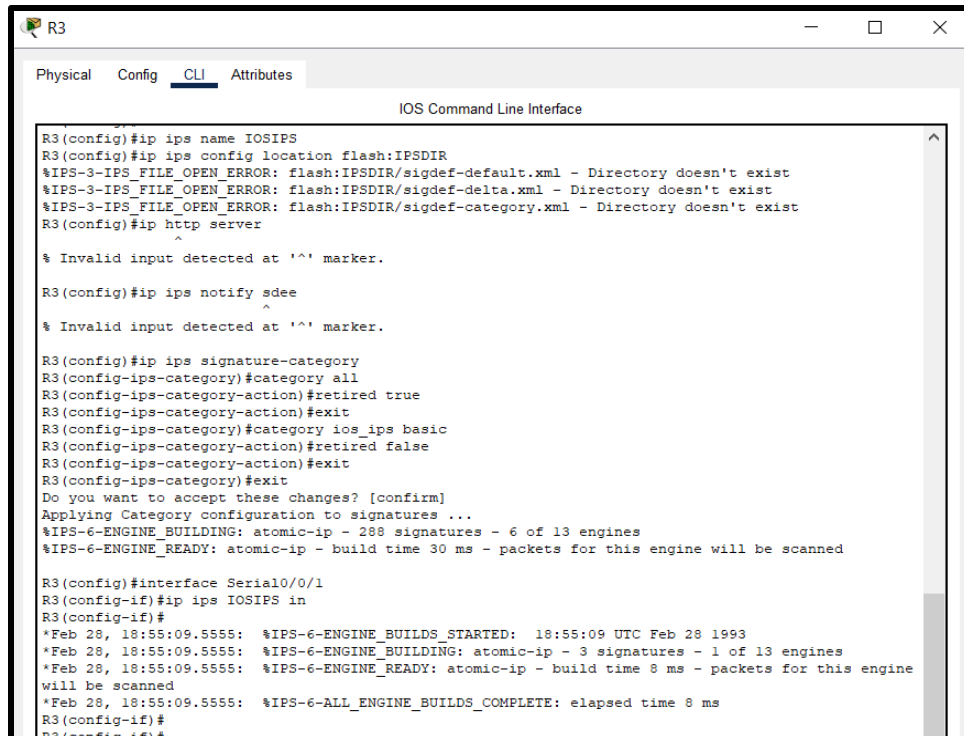
```
R1
Physical Config CLI Attributes
IOS Command Line Interface

R1#mkdir flash:IPSDIR
Create directory filename [IPSDIR]?
Created dir flash:IPSDIR

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip ips name IOSIPS
R1(config)#ip ips config location flash:IPSDIR
R1(config)#ip ips signature-category
R1(config-ips-category)#category all
R1(config-ips-category-action)#retired true
R1(config-ips-category-action)#exit
R1(config-ips-category)#category ios_ips basic
R1(config-ips-category-action)#retired false
R1(config-ips-category-action)#exit
R1(config-ips-category)#exit
Do you want to accept these changes? [confirm]
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this engine will be scanned

R1(config)#interface serial0/0/0
R1(config-if)#ip ips IOSIPS in
R1(config-if)#
*Feb 28, 19:09:17.099: %IPS-6-ENGINE_BUILDS_STARTED: 19:09:17 UTC Feb 28 1993
*Feb 28, 19:09:17.099: %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
*Feb 28, 19:09:17.099: %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this engine
will be scanned
*Feb 28, 19:09:17.099: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms
R1(config-if)#
```

The same configuration for the intrusion prevention system on the router R3 is also performed and the entire configuration is shown in the screenshot attached below.

A screenshot of the Cisco IOS CLI for router R3. The interface shows the configuration of an IPS named 'IOSIPS'. The configuration includes setting the location to 'flash:IPSDIR', defining three signature categories (default, delta, and category), and applying the category configuration to signatures. The output shows the configuration is applied successfully, with details about the number of signatures and the build time for each engine.

```
R3
Physical Config CLI Attributes
IOS Command Line Interface
R3(config)#ip ips name IOSIPS
R3(config)#ip ips config location flash:IPSDIR
%IPS-3-IPS_FILE_OPEN_ERROR: flash:IPSDIR/sigdef-default.xml - Directory doesn't exist
%IPS-3-IPS_FILE_OPEN_ERROR: flash:IPSDIR/sigdef-delta.xml - Directory doesn't exist
%IPS-3-IPS_FILE_OPEN_ERROR: flash:IPSDIR/sigdef-category.xml - Directory doesn't exist
R3(config)#ip http server
^
% Invalid input detected at '^' marker.
R3(config)#ip ips notify sdee
^
% Invalid input detected at '^' marker.
R3(config)#ip ips signature-category
R3(config-ips-category)#category all
R3(config-ips-category-action)#retired true
R3(config-ips-category-action)#exit
R3(config-ips-category)#category ios_ips basic
R3(config-ips-category-action)#retired false
R3(config-ips-category-action)#exit
R3(config-ips-category)#exit
Do you want to accept these changes? [confirm]
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this engine will be scanned
R3(config)#interface Serial0/0/1
R3(config-if)#ip ips IOSIPS in
R3(config-if)#
*Feb 28, 18:55:09.5555: %IPS-6-ENGINE_BUILDS_STARTED: 18:55:09 UTC Feb 28 1993
*Feb 28, 18:55:09.5555: %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
*Feb 28, 18:55:09.5555: %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this engine will be scanned
*Feb 28, 18:55:09.5555: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms
R3(config-if)#
R3(config-if)#
```

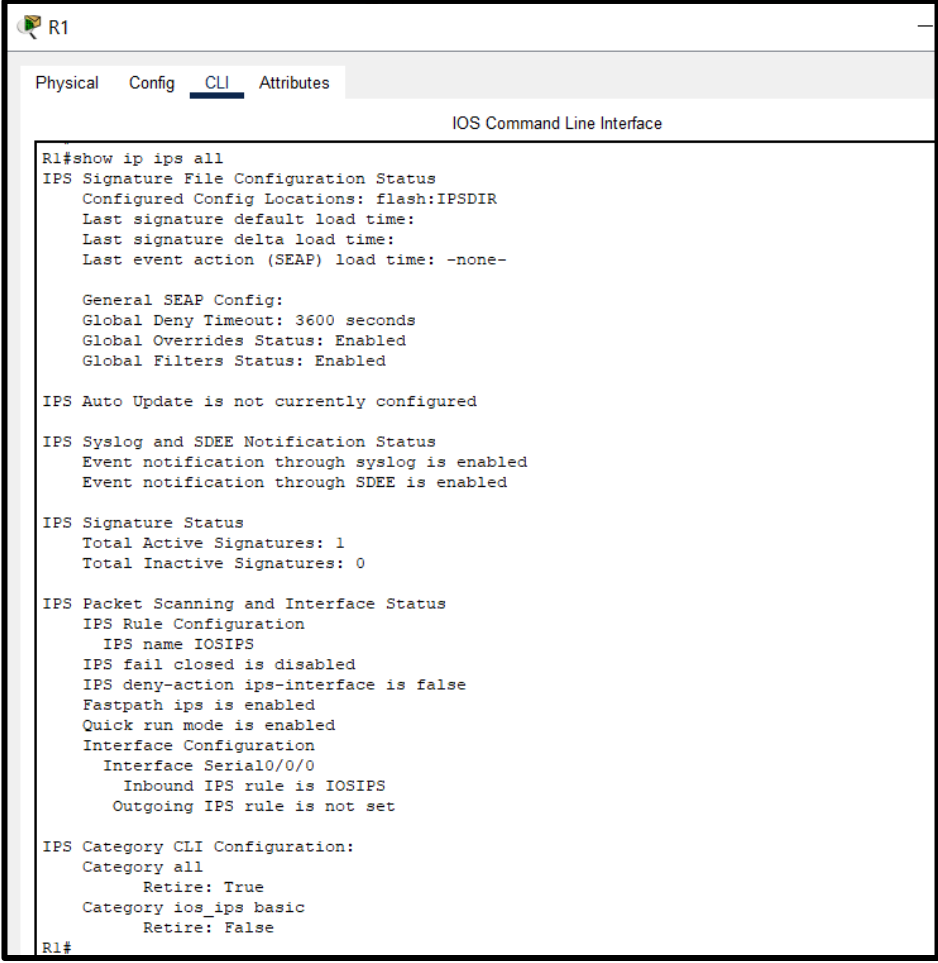
4.9.4. Verify Cisco IOS IPS operations

The next step is to proceed with verification of Cisco IOS IPS operations and it will be done on all routers. In the case of router R1, the use of show IPS signature count command is executed that shows out the entire configuration.

A screenshot of the Cisco IOS CLI for router R1. The user has entered the command 'show ip ips signatures count'. The output displays the Cisco SDF release version (S339.0), the Trend SDF release version (V0.0), and the signature micro-engine configuration. It shows that there is 1 total signature, 0 enabled signatures, 0 retired signatures, and 1 compiled signature.

```
R1
Physical Config CLI Attributes
IOS Command Line Interface
R1#show ip ips signatures count
Cisco SDF release version S339.0
Trend SDF release version V0.0
Signature Micro-Engine: string-icmp: Total Signatures 1
string-icmp enabled signatures: 0
string-icmp retired signatures: 1
Total Signatures: 1
Total Enabled Signatures: 0
Total Retired Signatures: 0
Total Compiled Signatures: 1
R1#
R1#
R1#
```

On the router R1 console, the show all command is also executed that shows all prevention configurations made that will assure that network is protected from all sort of cyber threats.



```
R1#show ip ips all
IPS Signature File Configuration Status
  Configured Config Locations: flash:IPSDIR
  Last signature default load time:
  Last signature delta load time:
  Last event action (SEAP) load time: -none-

  General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
  Event notification through syslog is enabled
  Event notification through SDEE is enabled

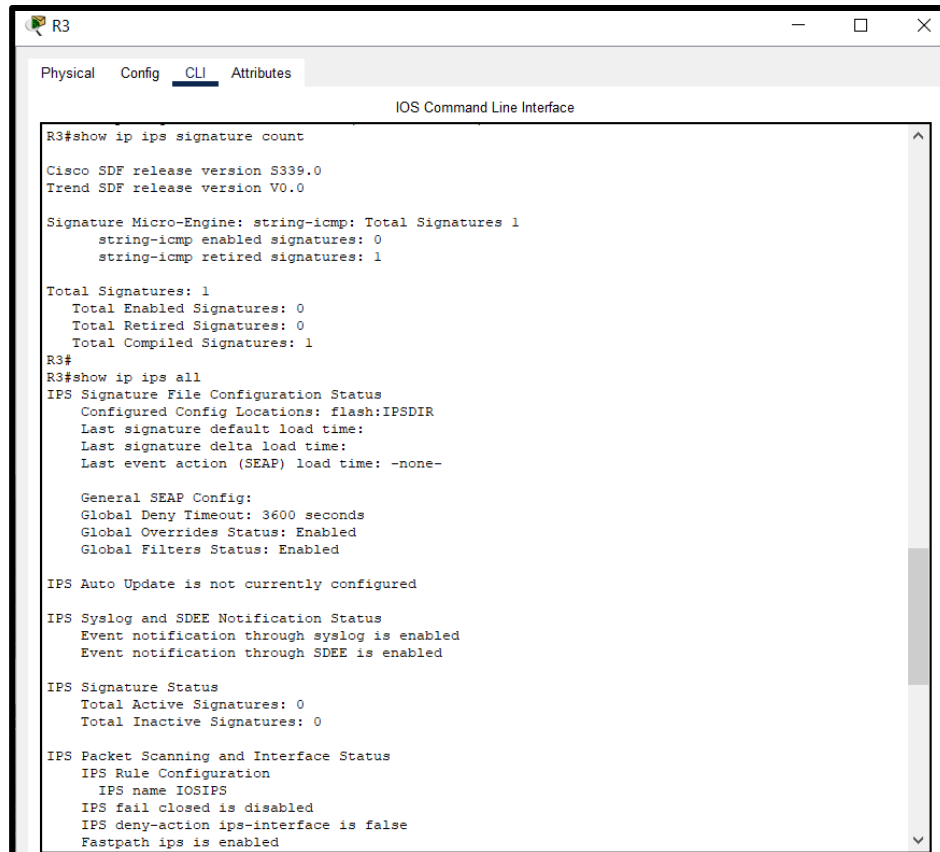
IPS Signature Status
  Total Active Signatures: 1
  Total Inactive Signatures: 0

IPS Packet Scanning and Interface Status
  IPS Rule Configuration
    IPS name IOSIPS
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Fastpath ips is enabled
    Quick run mode is enabled
  Interface Configuration
    Interface Serial0/0/0
      Inbound IPS rule is IOSIPS
      Outgoing IPS rule is not set

IPS Category CLI Configuration:
  Category all
    Retire: True
  Category ios_ips basic
    Retire: False

R1#
```

All the configurations made to the routers are checked using show command and in the case of router R3 also, the same command is issued to verify the connections.

A screenshot of a Cisco IOS Command Line Interface (CLI) window. The window has a title bar with 'R3' and standard window controls. Below the title bar are tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' being the active tab. The main area displays the output of two commands: 'show ip ips signature count' and 'show ip ips all'. The output shows various IPS statistics and configuration details.

```
R3#show ip ips signature count
Cisco SDF release version S339.0
Trend SDF release version V0.0

Signature Micro-Engine: string-icmp: Total Signatures 1
    string-icmp enabled signatures: 0
    string-icmp retired signatures: 1

Total Signatures: 1
Total Enabled Signatures: 0
Total Retired Signatures: 0
Total Compiled Signatures: 1
R3#
R3#show ip ips all
IPS Signature File Configuration Status
  Configured Config Locations: flash:IPSDIR
  Last signature default load time:
  Last signature delta load time:
  Last event action (SEAP) load time: -none-

General SEAP Config:
  Global Deny Timeout: 3600 seconds
  Global Overrides Status: Enabled
  Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
  Event notification through syslog is enabled
  Event notification through SDEE is enabled

IPS Signature Status
  Total Active Signatures: 0
  Total Inactive Signatures: 0

IPS Packet Scanning and Interface Status
  IPS Rule Configuration
    IPS name IOSIPS
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Fastpath ips is enabled
```

4.10.PART 9: IMPLEMENT A SITE-TO-SITE VPN

4.10.1.Purpose of VPNs

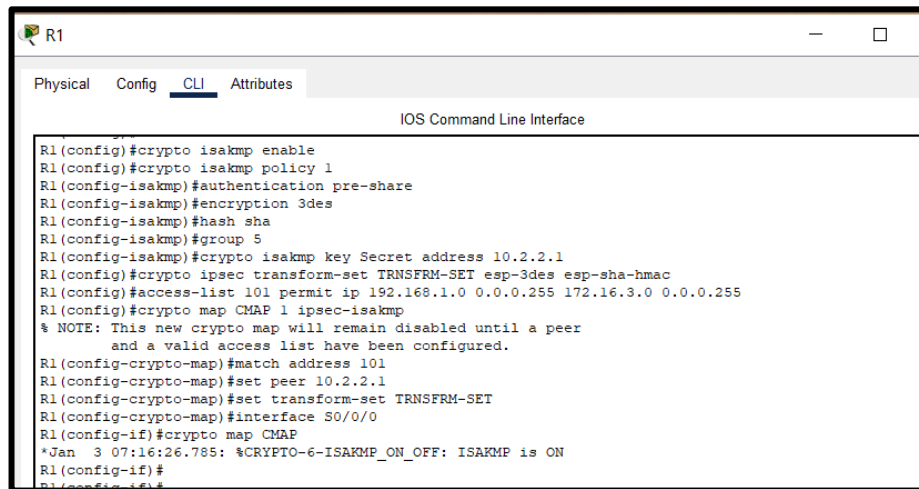
A VPN or Virtual Private Network, is a secure and encrypted internet connection that connects two devices. VPNs enable remote workers to safely access their organization's network from anywhere in the globe. VPNs can also be used to circumvent government censorship and gain access to prohibited information. A VPN conceals a user's internet traffic from their ISP, government or any other third party who may be monitoring their online activities. Lastly, the VPN can be used to securely share files between two devices connected to the internet (Firdaouss et al., 2022).

4.10.2.IPsec VPNs

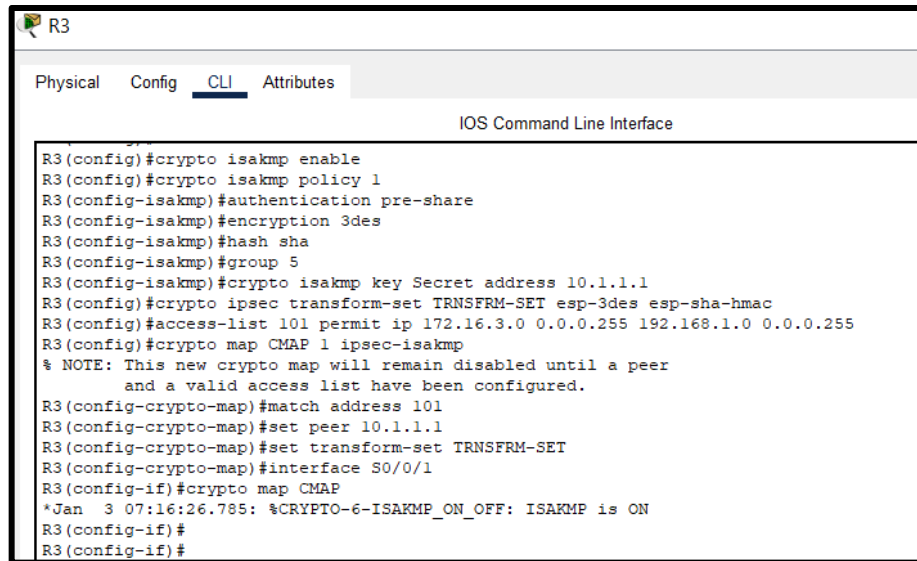
IPsec, which stands for Internet Protocol Security, is a protocol suite used to secure internet connections. This protocol suite is used by IPsec VPNs to facilitate secure communication between two devices over the internet. An IPsec VPN works by establishing a secure tunnel between two devices that require communication.

4.10.3.Configure a site-to-site IPsec VPN

As discussed earlier, the use of IPsec VPN is mainly done to make sure data transmission takes place between multiple sites in an easy manner. In the screenshot attached below, the configuration for the router R1 is shown where ISAKMP was enabled, policy was applied, encryption algorithm was defined, hashing algorithm was defined and other access control rules were formulated. In addition to this, peers and transform set is also defined along with serial interface (Firdaouss et al., 2022).

The image is a screenshot of a network simulator window titled 'R1'. It shows the 'CLI' (Command Line Interface) tab selected, displaying the 'IOS Command Line Interface'. The configuration commands entered are as follows:

```
R1(config)#crypto isakmp enable
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#hash sha
R1(config-isakmp)#group 5
R1(config-isakmp)#crypto isakmp key Secret address 10.2.2.1
R1(config)#crypto ipsec transform-set TRNSFRM-SET esp-3des esp-sha-hmac
R1(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 172.16.3.0 0.0.0.255
R1(config)#crypto map CMAP 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R1(config-crypto-map)#match address 101
R1(config-crypto-map)#set peer 10.2.2.1
R1(config-crypto-map)#set transform-set TRNSFRM-SET
R1(config-crypto-map)#interface S0/0/0
R1(config-if)#crypto map CMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
```



```
R3
Physical Config CLI Attributes
IOS Command Line Interface
R3(config)#crypto isakmp enable
R3(config)#crypto isakmp policy 1
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#encryption 3des
R3(config-isakmp)#hash sha
R3(config-isakmp)#group 5
R3(config-isakmp)#crypto isakmp key Secret address 10.1.1.1
R3(config)#crypto ipsec transform-set TRNSFRM-SET esp-3des esp-sha-hmac
R3(config)#access-list 101 permit ip 172.16.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#crypto map CMAP 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)#match address 101
R3(config-crypto-map)#set peer 10.1.1.1
R3(config-crypto-map)#set transform-set TRNSFRM-SET
R3(config-crypto-map)#interface S0/0/1
R3(config-if)#crypto map CMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#
```

4.10.4. Description to Encryption, Hashes, and Digital Signatures for CIA

Cryptographic techniques such as encryption, hashing and digital signatures are all used to provide various levels of security. They can provide confidentiality, integrity and authentication when used collectively. Data confidentiality is achieved through the use of encryption. When data is encrypted, it is scrambled so that it can only be read by those who have the encryption key. This ensures that even if the data is intercepted, no one who does not have the key may read it. Hashes are used to confirm that no data has been tampered with. A hash is a mathematical function that takes in data and returns a string of characters of a specific length. If the data is altered in any manner, the hash will be altered as well. The receiver can confirm that the data has not been tampered with by comparing the hash of the original data to the hash of the received data. If the two hashes match, the recipient knows the data came from the sender and was not tampered (Firdaouss et al., 2022).

4.10.5. Use of Cryptographic hashes

Cryptographic hashes are one-way mathematical functions that accept a message or data as input and output a fixed-length string of characters. The hash function

protects data by creating a unique digital fingerprint or message digest from the input data. If even one bit of the input data changes, the resultant hash changes. As a result, the receiver can validate the data integrity by comparing the calculated hash of the received data to the predicted hash of the original data. Authentication is also done using cryptographic hashes. A sender can create a digital signature by hashing a message and then encrypting it using their private key.

4.10.6. Use of Encryption Algorithm

Data confidentiality is ensured by the use of encryption methods. Encryption is the process of converting plaintext into cipher text using an encryption key so that the original material may be read only by those who have the decryption key. The encryption and decryption processes provide data confidentiality and privacy. The encryption algorithm should be robust enough that unauthorized parties cannot decrypt the encrypted message.

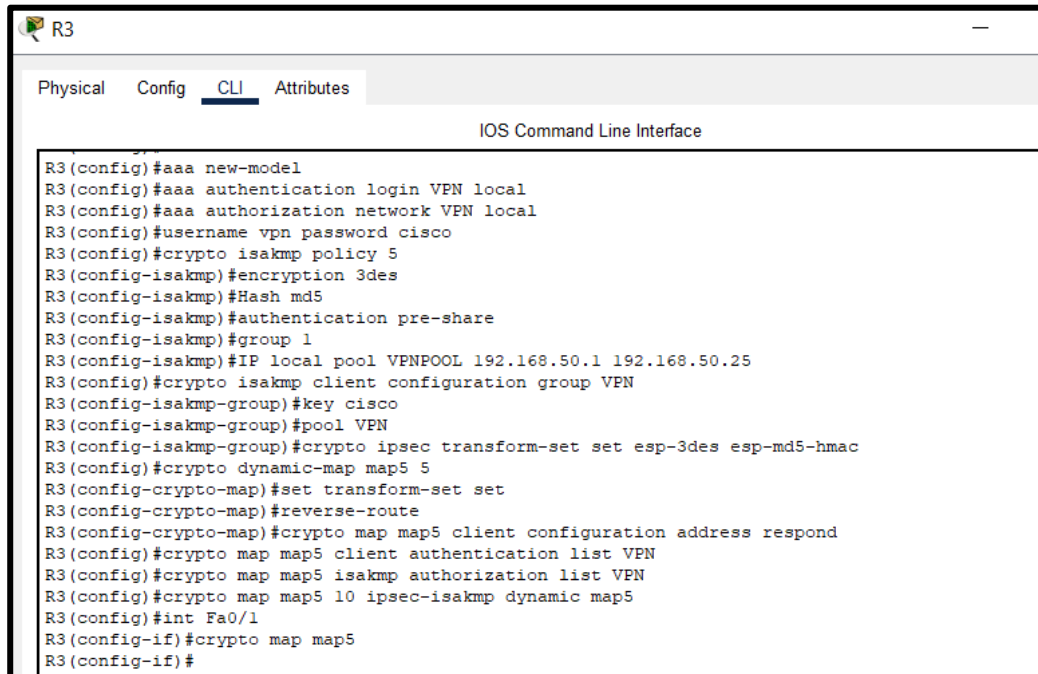
4.10.7. PKI Uses

A Public Key Infrastructure (PKI) is a system that provides confidentiality and authentication by utilizing public key cryptography and digital certificates. To validate their identity, the owner of the private key digitally signs a message in PKI. By decrypting the digital signature with the sender's public key, the recipient can confirm the sender's identity. PKI also ensures communication secrecy by encrypting messages with the receiver's public key, allowing only the recipient with their private key to decipher the message. Digital certificates are used to enable trustworthy third-party validation of the identity of a public key holder. This trusted validation allows the recipient to confirm the identity of the sender and establish safe communication channels (Zhai, Shen and Mao, 2022).

4.11.PART 10: IMPLEMENT A REMOTE ACCESS VPN.

4.11.1.Configure a Remote-access VPN

The configuration for the remote access VPN is now done on the router R3 and it is done by enabling AAA model, performing authentication, applying encryption protocols, keys, pools and many others.



```
R3
Physical Config CLI Attributes
IOS Command Line Interface
R3(config)#aaa new-model
R3(config)#aaa authentication login VPN local
R3(config)#aaa authorization network VPN local
R3(config)#username vpn password cisco
R3(config)#crypto isakmp policy 5
R3(config-isakmp)#encryption 3des
R3(config-isakmp)#hash md5
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 1
R3(config-isakmp)#IP local pool VPNPOOL 192.168.50.1 192.168.50.25
R3(config)#crypto isakmp client configuration group VPN
R3(config-isakmp-group)#key cisco
R3(config-isakmp-group)#pool VPN
R3(config-isakmp-group)#crypto ipsec transform-set set esp-3des esp-md5-hmac
R3(config)#crypto dynamic-map map5 5
R3(config-crypto-map)#set transform-set set
R3(config-crypto-map)#reverse-route
R3(config-crypto-map)#crypto map map5 client configuration address respond
R3(config)#crypto map map5 client authentication list VPN
R3(config)#crypto map map5 isakmp authorization list VPN
R3(config)#crypto map map5 10 ipsec-isakmp dynamic map5
R3(config)#int Fa0/1
R3(config-if)#crypto map map5
R3(config-if)#
```

4.11.2.Configure Remote-access VPNs on an ASA

The configuration for the remote access VPN is not possible on the ASA as the commands are not working on the Cisco Packet tracer software.

4.12.PART 11: DEPLOY THE CISCO ASA FOR FIREWALLING AND NAT/PAT SERVICES

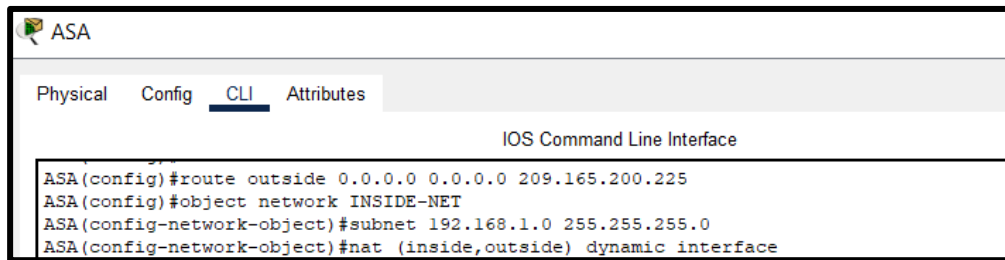
4.12.1.ASA Operating

Cisco Systems' Adaptive Security Appliance (ASA) is a stateful firewall that provides sophisticated security features and capability for network traffic filtering and protection. As a stateful firewall, the ASA keeps track of every connection

made between hosts on the network, allowing it to make more accurate judgments about whether to accept or block traffic depending on the connection's current state. This stateful inspection technology enables the ASA to distinguish between valid traffic that is part of an established connection and traffic that is not. Aside from the stateful inspection, the ASA has a number of sophisticated security features such as intrusion prevention, application level inspection and VPN capabilities.

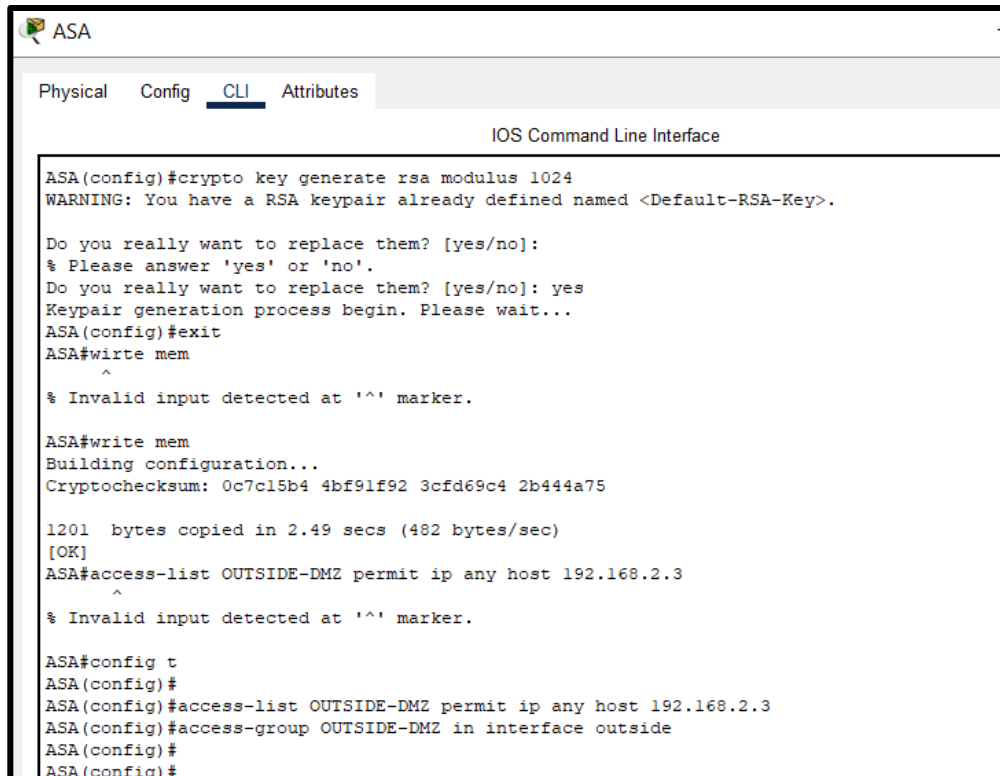
4.12.2.Implementing ASA firewall

Now, the implementation for the ASA Firewall is being done here the outside route has been assigned along with object as INSIDE-NET. In addition to this, the subnet details are also assigned on the ASA firewall (Zhai, Shen and Mao, 2022).



```
ASA
Physical Config CLI Attributes
IOS Command Line Interface
ASA(config)#route outside 0.0.0.0 0.0.0.0 209.165.200.225
ASA(config)#object network INSIDE-NET
ASA(config-network-object)#subnet 192.168.1.0 255.255.255.0
ASA(config-network-object)#nat (inside,outside) dynamic interface
```

Once the configuration is completed, the crypto key modulus is generated and access control lists are applied to make ASA firewall work efficiently.



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

ASA(config)#crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

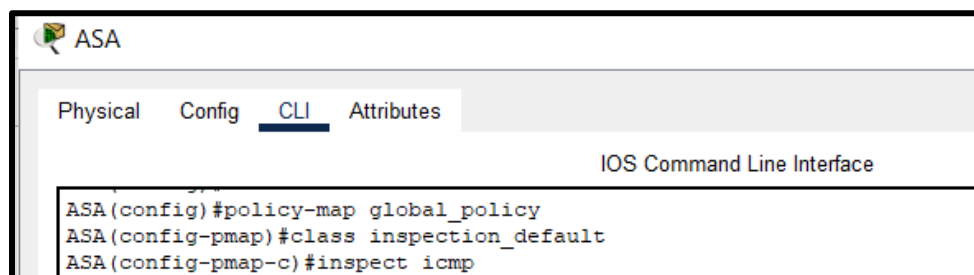
Do you really want to replace them? [yes/no]:
% Please answer 'yes' or 'no'.
Do you really want to replace them? [yes/no]: yes
Keypair generation process begin. Please wait...
ASA(config)#exit
ASA#write mem
^
% Invalid input detected at '^' marker.

ASA#write mem
Building configuration...
Cryptochecksum: 0c7c15b4 4bf91f92 3cfd69c4 2b444a75

1201 bytes copied in 2.49 secs (482 bytes/sec)
[OK]
ASA#access-list OUTSIDE-DMZ permit ip any host 192.168.2.3
^
% Invalid input detected at '^' marker.

ASA#config t
ASA(config)#
ASA(config)#access-list OUTSIDE-DMZ permit ip any host 192.168.2.3
ASA(config)#access-group OUTSIDE-DMZ in interface outside
ASA(config)#
ASA(config)#
```

Now, the policy map global policy command is executed and ICMP inspection is being made.



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

ASA(config)#policy-map global_policy
ASA(config-pmap)#class inspection_default
ASA(config-pmap-c)#inspect icmp
```

5. PART 2: PROPOSE A SECURE NETWORK INFRASTRUCTURE

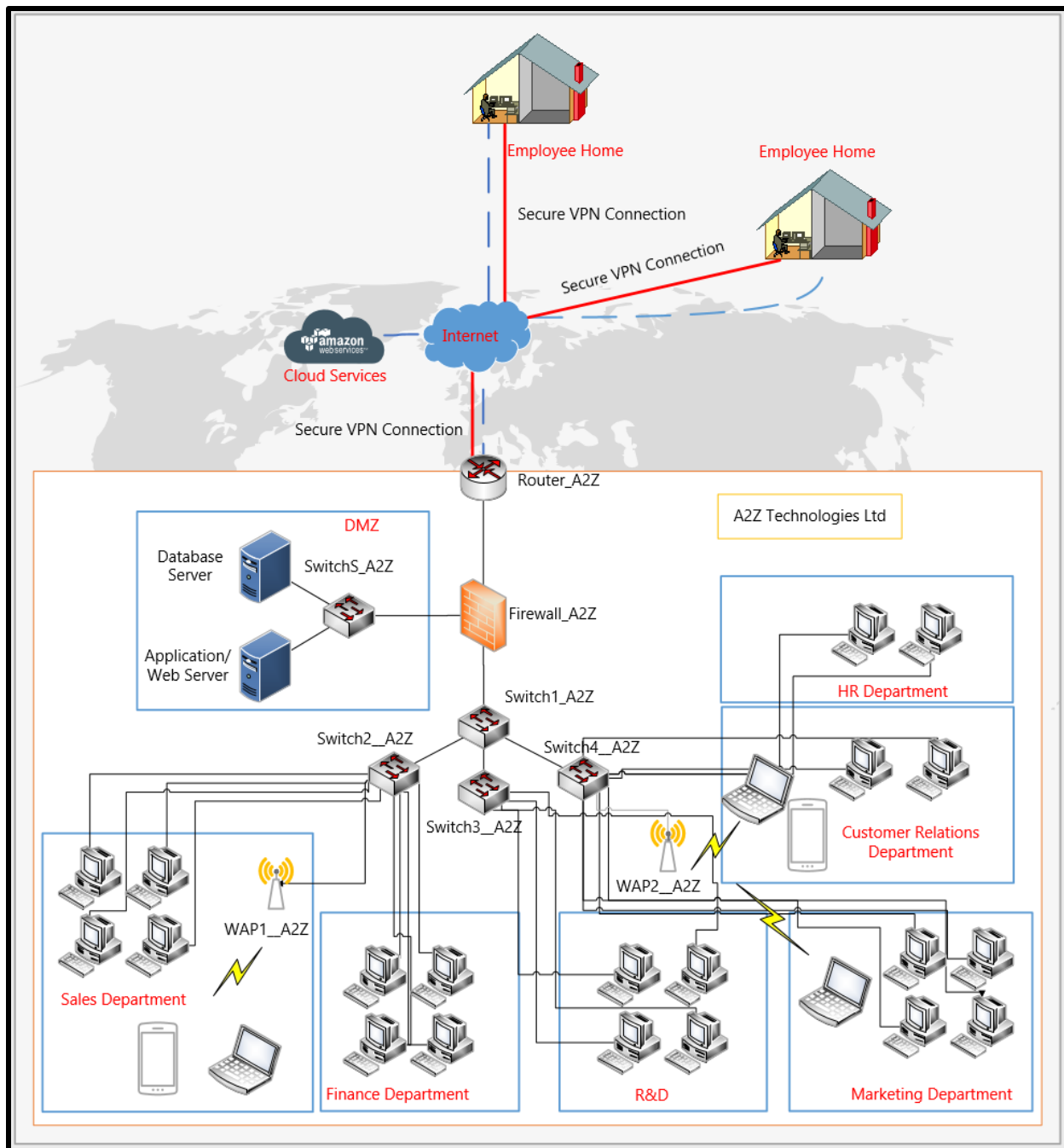
5.1. INTRODUCTION TO THE SCENARIO

The given scenario is based on designing a secure network infrastructure for the A2Z Technologies Ltd. This company is headquartered in Swansea and is specialized in designing and manufacturing high tech electronic equipment which are then sold to retailing companies. The company's manufacturing plant is located

at Cardiff. Mainly, the head office comprises of Sales department, HR department, finance department, marketing department, customer relations department and R&D. The main aim of the company is to make their network infrastructure secure to make sure they can mitigate all sort of cyber threats. Even though workers who are working from the home must be allowed to access company's resources virtually. The organization has even adopted some cloud services and is allowing their devices to perform their actions on a daily basis.

5.2. NETWORK BLUE PRINT

The network design given below shows the layout for the A2Z network, including device placement and interconnectivity.



5.3. JUSTIFICATION OF NETWORK DESIGN

In the above attached network design, all A2Z organization's technical and business requirements are taken into consideration to propose a secure network infrastructure. At the network border, the main router has been configured that connects with the internet service provider. Through external network connectivity,

cloud services are also used by the organization to carry out their business operations in a daily routine. In addition to this, employees who are working from the home can also connect to the organizational network securely via secure VPN connection. Using secure VPN connection, a tunnel is established that securely connects the employee to the organizational network. From the internal network, the main router directly connects with the firewall where firewall further has two allocated ports. The first port is for the DMZ area where database and application/web server are configured and placed in an isolated place. On the other hand, the second port is protecting internal network where all departments are connected. The main switch connects to different switches and wireless access points in order to make sure all other departments are able to access network resources via wired and wireless connections (Stokel-Walker, 2021).

5.4. PROPOSED CHOICES AND SECURITY MEASURES

Referring to the given network design architecture for the A2Z organization, the following are some proposed choices, including security measures to protect organizational network from possible cyber-attacks.

1. On the basis of given requirements, there will be a need for a network firewall which will be placed between the internal network and a main router to make sure all incoming traffic is investigated to avoid risks of facing unavailability attacks.
2. For the purpose of securing internal LAN from possible cyber-attacks, the DMZ zone is created for servers which will make sure public traffic can come until DMZ zone.
3. Another proposed choice is to implement encryption and access control feature on the network devices to assure only network administrator is able to access root mode of all devices.

4. For remote connectivity and to securely allow employees to connect with the organizational network, the use of virtual private network (VPN) is required for secure data transmission.
5. For wireless security, all wireless access points (WAPs) are required to have WPA2-PSK protocol to assure only authorized ones are able to access the organizational network wirelessly (Stokel-Walker, 2021).
6. The major proposed choice is to integrate cloud based services like Azure active directory, virtual machines, content delivery networks, SQL servers, and many more to lessen on-site maintenance.

5.5. PROPOSED COST ANALYSIS

5.5.1. Vendor 1

Vendor	Device	Model	Specification	Cost
CISCO	Router	Cisco ISR 4331 - Router	Enclosure Type: - Rack-mountable - modular - 1U Connectivity Technology: - Wired Data Link Protocol: - Ethernet, Fast Ethernet, Gigabit Ethernet Performance Aggregate throughput: - 100 Mbps Network / Transport Protocol/IPSec, PPPoE, DHCP	£1,679.67
CISCO	Firewall	Cisco ASA 5525-X Firewall Edition Security Appliance 8 Ports 1U	Form Factor: - Rack-mountable - 1U RAM: - 12 GB Ports Qty:- 8 Data Link Protocol: - Gigabit Ethernet Performance Firewall throughput: - 2 Gbps , VPN throughput (3DES/AES): 300 Mbps , Connection rate: 20000 connections per second , Firewall + intrusion prevention throughput: 600 Mbps	£5,360.99

CISCO	Switch	6. CISCO SG250- 26P 26 PORT SWITCH	Enclosure Type:- Rack-mountable 1U Subtype Gigabit Ethernet Ports:- 24 x 10/100/1000 (PoE+) + 2 x combo Gigabit SFP	£387.79
CISCO	Wireless Access Point	Cisco Aironet 2802E Radio Access Point 802.11ac	Product Description: - Cisco Aironet 2802E - radio access point - Wi-Fi 5	£1,239.07

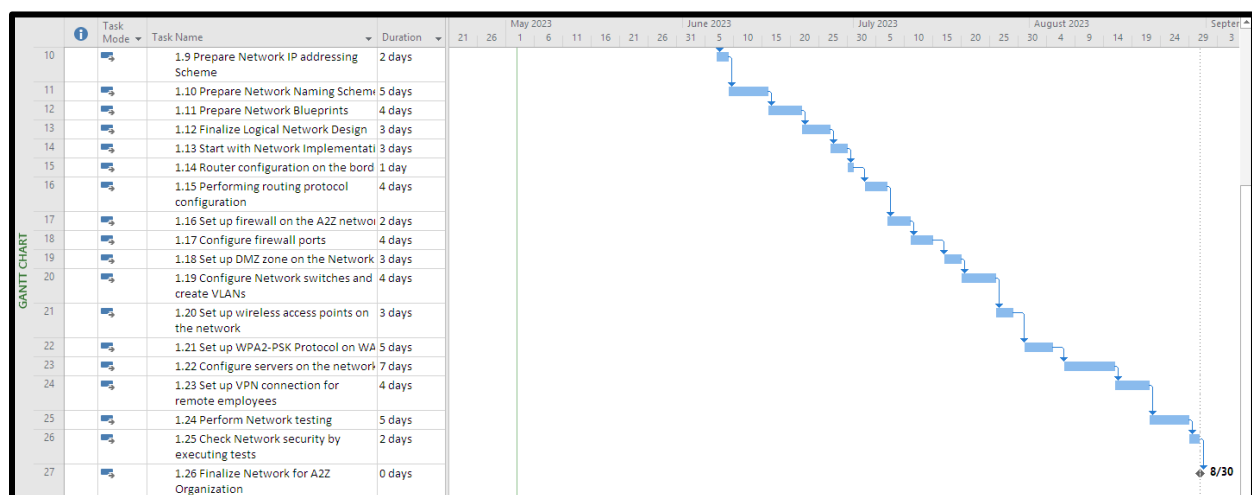
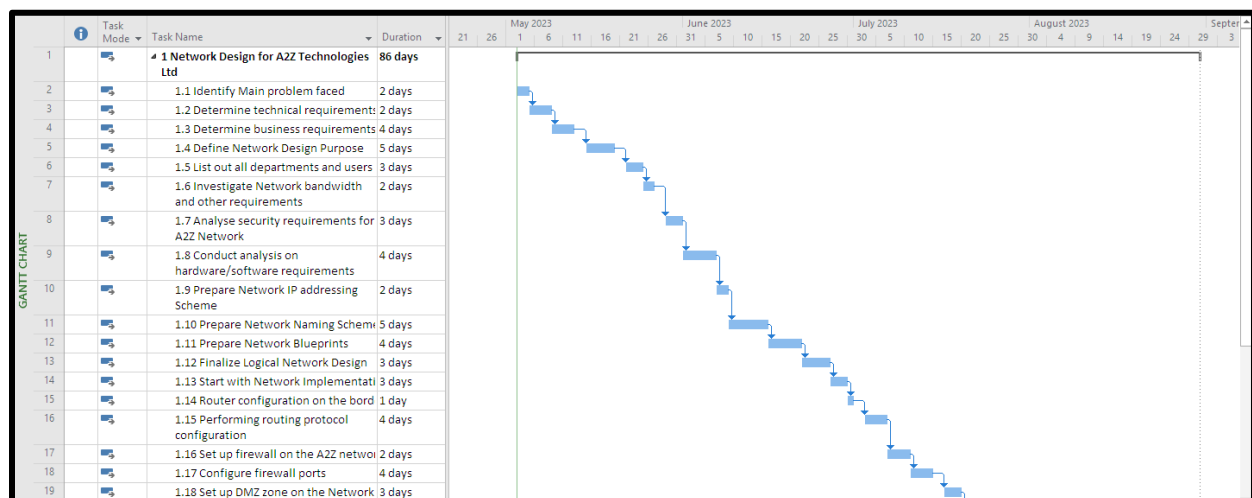
5.5.1. Vendor 2

Vendor	Device	Model	Specifications	Cost
Ubiquiti	Router	AR2240C-S - Huawei AR2200 Series Router	Huawei Enterprise 10/100/1000 Router, 3GE WAN (2 Combo), 2G Memory	£1,200.97
Ubiquiti	Firewall	S2720-28TP-PWR- EI	S2720-28TP- PWR-EI - Huawei S2720-EI Enterprise Switches	£448.00
Ubiquiti	Switch	Ubiquiti UniFi Switch US-24	Product Description Ubiquiti UniFi Switch US-24-250W - switch - 24 ports - Managed - rack-mountable Device Type Switch - 24 ports - Managed Enclosure Type Rack-mountable 1U Subtype Gigabit Ethernet Ports 24 x 10/100/1000 (PoE+) + 2 x Gigabit SFP	

Ubiquiti	Wireless Access Point	Ubiquiti Networks WLAN Access Point 5 Pack	Product Description: - Ubiquiti UniFi AP-AC Pro - radio access point - Wi-Fi 5 Frequency Band: - 2.4 GHz, 5 GHz	£602.71
----------	--------------------------	--	--	---------

5.7. PROJECT PLAN

The timeline prepared for the A2Z network implementation project is provided below with respect to start date, end date and total duration.



5.8. POSSIBLE ATTACKS

Even after implementing network security systems, there are chances for facing severe attacks, some of them are explained below in a detailed manner.

- **DDoS attack:** The A2Z technologies can face the DDoS attack on their network infrastructure even after setting up a firewall due to dynamic nature of DDoS attempts. The main purpose of executing this attack will be disrupting the normal traffic flow by overwhelming the network with a flood of traffic from the multiple sources to avoid other users to access network services. Therefore, there is a major requirement for further planning to make sure A2Z network remain protected from all types of attacks (Dayal and Srivastava, 2023).
- **SQL Injection:** The next type of attack that could be faced on the network is SQL injection on the database server. Under this attack, the attacker will try to exploit A2Z database by executing malicious SQL queries which generated an error despite revealing internal information to cyber attackers. There are higher chances for facing SQL injection attack if no prepared statements are used on the database.
- **Ransomware attack:** One of the most perilous attacks that can be faced by the A2Z organization's network is ransomware. Under this type of attack, the use of asymmetric algorithms is done which encrypts entire infrastructure with random extension to make files inaccessible to other users. This also provides a lock out where a ransom amount is to be paid to the attacker via crypto currency.
- **Man-in-the-middle:** This attack can be implemented on the A2Z technologies when the traffic is being transmitted between the networks. The malicious parties intercept that traffic between the networks. This attack over the A2Z technologies can be successful if the company has weak

security protocols like WPA2 which has been used on the wireless network (Dayal and Srivastava, 2023).

5.9. RECOMMENDED TESTS

The given below are three different types of tests that are required for the A2Z organizational network.

- The first type of test that is required once the implementation is over is accessibility in order to make sure all services works perfectly.
- From the security point of view, there is also a need for conducting gray box testing to test all services to assure a secure environment is maintained.
- The last type of test that is recommended for the organizational network is performance test that will help in identifying network performance based on bandwidth, jitter and latency.

5.10.COST FOR IMPLEMENTATION

The final cost for the secure network implementation would be \$1,00,000.

6. CONCLUSION

From the above report, it can be said that there is a major need for setting up a secure network environment in order to make sure all business operations remain protected from possible cyber-attacks. The first task performed in this report is based on completing all labs that are associated with the Cisco packet tracer simulation software. All labs were completed which were related to secure configuration of network components. After this, the second part is based on proposing a network design to the organization. The secure design is proposed based on given requirements and a detailed discussion on testing and security requirements has also been done.

7. REFERENCES

- Agar, D., Grgić, K. and Rimac-Drlje, S. (2007) "Security aspects in IPv6 networks – implementation and testing," *Computers & Electrical Engineering*, 33(5–6), pp. 425–437. Available at: <https://doi.org/10.1016/j.compeleceng.2007.05.008>.
- Amal and Venkadesh, P. (2023) "H-DOCTOR: Honeypot based firewall tuning for attack prevention," *Measurement: Sensors*, 25, p. 100664. Available at: <https://doi.org/10.1016/j.measen.2022.100664>.
- Chow, S.S.M. *et al.* (2005) "A generic anti-spyware solution by access control list at kernel level," *Journal of Systems and Software*, 75(1–2), pp. 227–234. Available at: <https://doi.org/10.1016/j.jss.2004.05.027>.
- Dayal, N. and Srivastava, S. (2023) "Analyzing Effective Mitigation of DDoS Attack with Software Defined Networking," *Computers & Security*, 130, p. 103269. Available at: <https://doi.org/10.1016/j.cose.2023.103269>.
- Firdaouss, L. *et al.* (2022) "Automated VPN configuration using DevOps," *Procedia Computer Science*, 198, pp. 632–637. Available at: <https://doi.org/10.1016/j.procs.2021.12.298>.
- Liu, D., Barber, B.K. and DiGrande, L. (2009) "VLAN Trunking Protocol," in *Elsevier eBooks*. Elsevier BV, pp. 575–596. Available at: <https://doi.org/10.1016/b978-1-59749-306-2.00018-x>.
- Sari, L.S.N. *et al.* (2018) "A Comparison between the Use of Cisco Packet Tracer and Graphical Network Simulator 3 as Learning Media on Students' Achievement," *Jurnal Pendidikan Teknologi Dan Kejuruan*, 24(1), pp. 132–136. Available at: <https://doi.org/10.21831/jptk.v24i1.16042>.
- Song, M., Wang, L. and Song, J. (2008) "A secure fast handover scheme based on AAA protocol in mobile IPv6 networks," *The Journal of China Universities of Posts and Telecommunications* [Preprint]. Available at: [https://doi.org/10.1016/s1005-8885\(08\)60147-8](https://doi.org/10.1016/s1005-8885(08)60147-8).
- Stokel-Walker, C. (2021) "VPN flaw could put users at risk," *New Scientist*, 251(3348), p. 10. Available at: [https://doi.org/10.1016/s0262-4079\(21\)01444-5](https://doi.org/10.1016/s0262-4079(21)01444-5).

- Wang, X., Yu, L. and Li, J. (2023) “Relationships between childhood maltreatment, attachment security, and features of narcissism: A network analysis,” *Personality and Individual Differences*, 200, p. 111890. Available at: <https://doi.org/10.1016/j.paid.2022.111890>.
- Wu, W., Qi, Q. and Yu, X. (2023) “Deep learning-based data privacy protection in software-defined industrial networking,” *Computers & Electrical Engineering*, 106, p. 108578. Available at: <https://doi.org/10.1016/j.compeleceng.2023.108578>.
- Xiong, P. *et al.* (2023) “Backup protection method based on multi-interval information in low voltage distribution network of high proportion of renewable energy system,” *Energy Reports*, 9, pp. 487–494. Available at: <https://doi.org/10.1016/j.egyr.2023.01.058>.
- Zhai, Z., Shen, S. and Mao, Y. (2022) “BPKI: A secure and scalable blockchain-based public key infrastructure system for web services,” *Journal of Information Security and Applications*, 68, p. 103226. Available at: <https://doi.org/10.1016/j.jisa.2022.103226>.