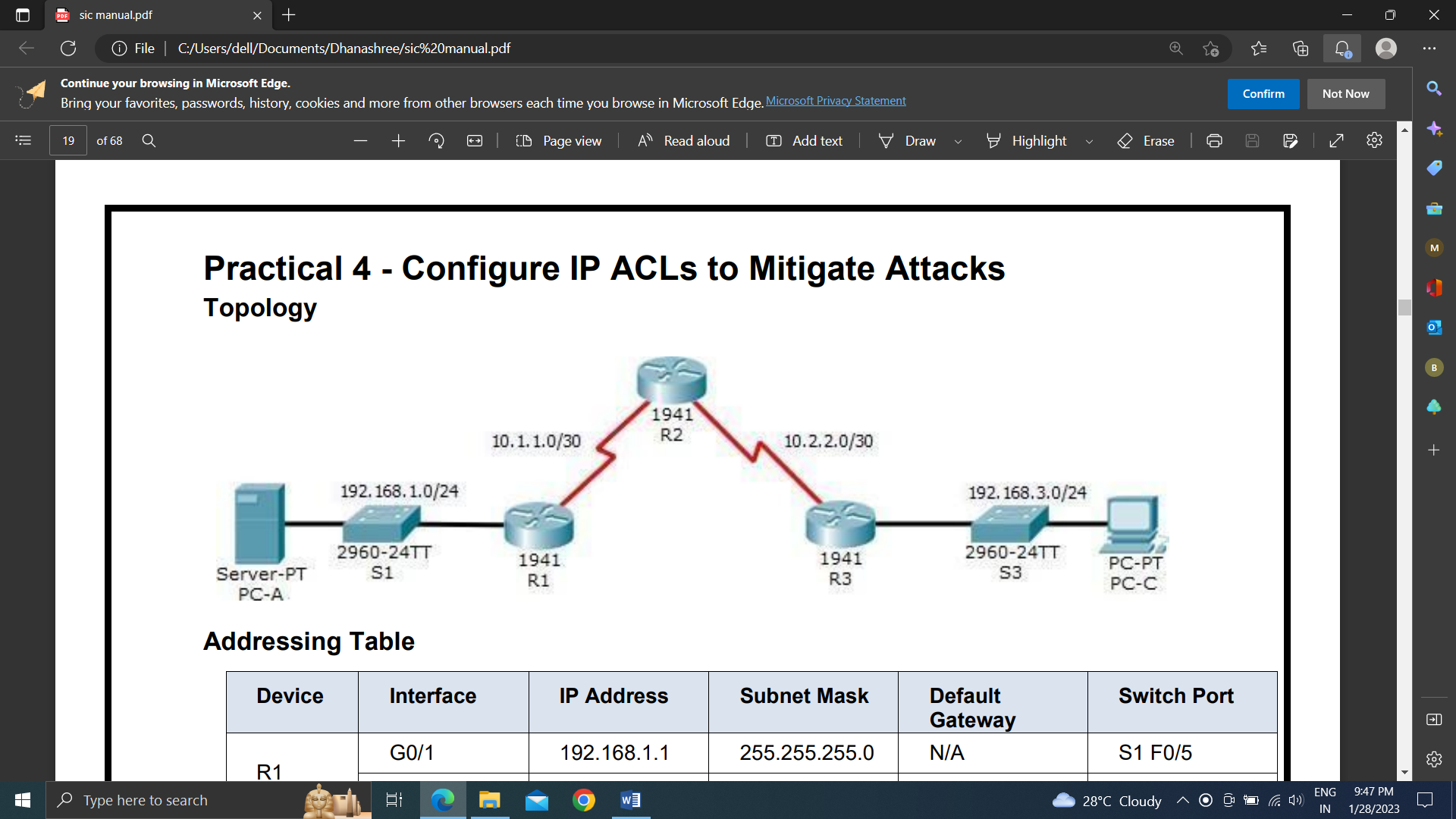
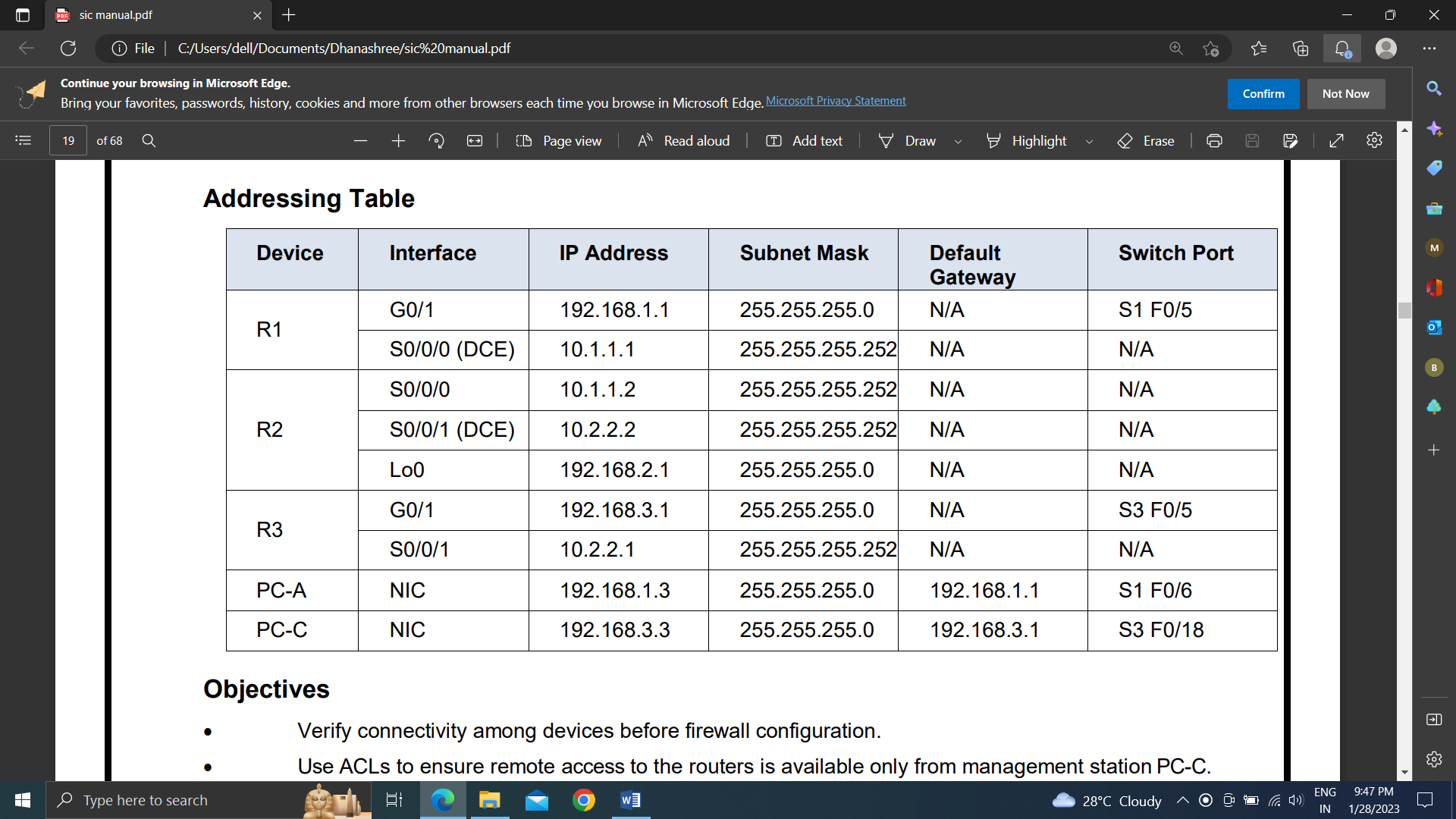
**Practical No:-4**

**Aim:-**  **Configure IP ACLs to Mitigate Attacks.**

**Solution:-**





The routers have been pre-configured with the following:

* Enable password: skcenpa55
* Password for console: skcconpa55
* SSH logon username and password: SSHadmin/skcsshpa55
* IP addressing
* Static routing

**For all Routers**

R0UTER(config)#enable password ciscoenpa55

R0UTER(config)#line console 0

R0UTER(config-line)#password ciscoconpa55

R0UTER(config-line)#exit

R0UTER(config)#username SSHadmin password ciscosshpa55

R0UTER(config)#

To ADD Loopback interface address in R2

R2(config)#interface loopback 0

R2(config-if)#ip address 192.168.2.1 255.255.255.0

R2(config-if)#exit

R2(config)#

**For R1**

R1> enable

R1#config t

R1(config)# router ospf 1

R1(config-router)# network 10.1.1.0 0.0.0.3 area 0

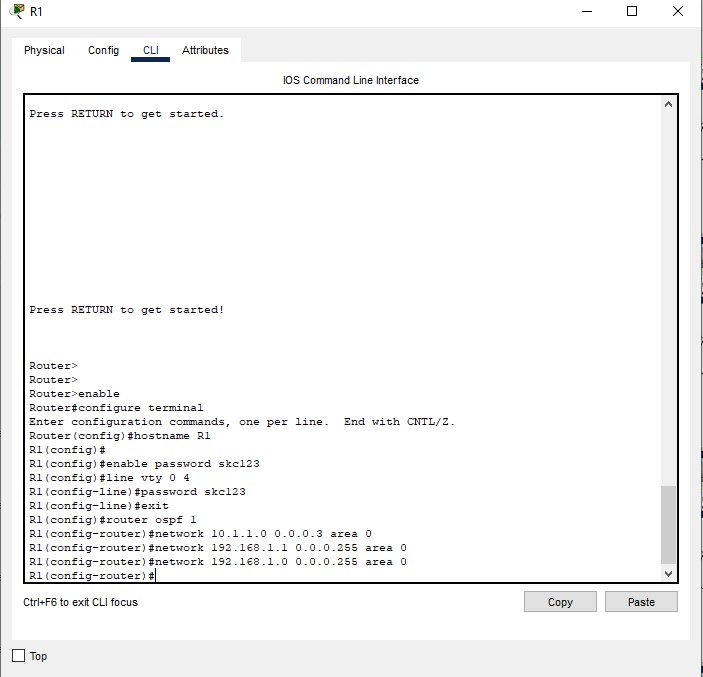
R1(config-router)# network 192.168.1.1 0.0.0.255 area 0

R1(config-router)# Exit

R1(config)# exit

Use following command to verify that OSPF has neighbours.

R1# show ip ospf neighbour



**Experiment No: Class: TYIT**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**For R2**

R2> enable

R2#config t

R2(config)# router ospf 1

R2(config-router)# network 10.1.1.0 0.0.0.3 area 0 R2(config-router)# network 10.2.2.0 0.0.0.3 area 0

R2(config-router)# Exit

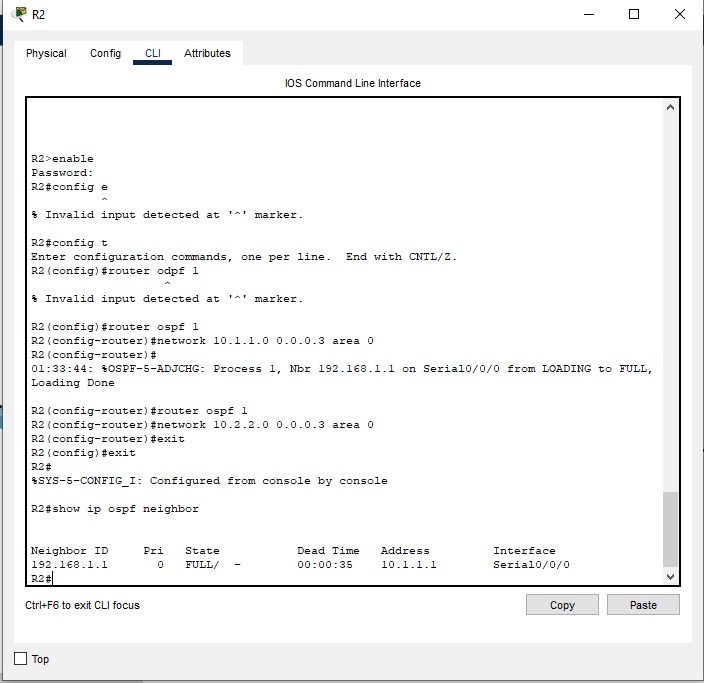
R2(config)# exit

Use following command to verify that OSPF has neighbours.

R2# show ip

ospf

neighbor



**Experiment No: Class: TYIT**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**For R3**

R3> enable

R3#config t

R3(config)# router ospf 1

R3(config-router)# network 10.2.2.0 0.0.0.3 area 0

R3(config-router)# network 192.168.3.0 0.0.0.255 area 0

R3(config-router)# Exit

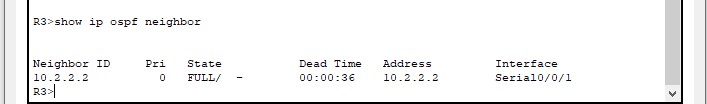
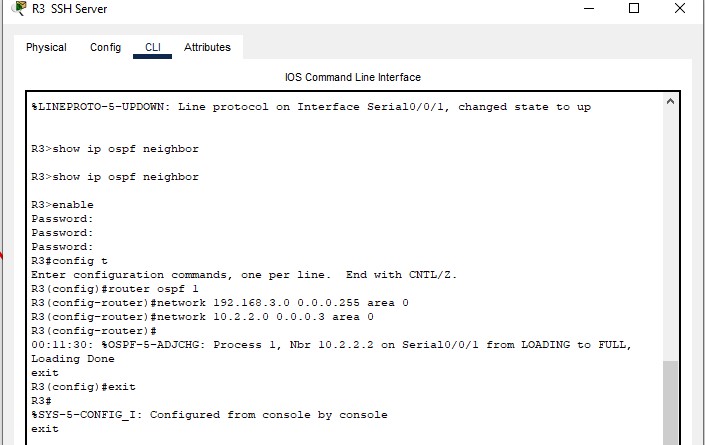
R3(config)# exit

Use following command to verify that OSPF has neighbours.

R3# show ip

ospf

neighbor



**Experiment No: Class: TYIT**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Part 1: Configure OSPF MD5 Authentication**

**Step 1: Test connectivity. All devices should be able to ping all other IP addresses.**

**Step 2: Configure OSPF MD5 authentication for all the routers in area 0.**

Configure OSPF MD5 authentication for all the routers in area 0.

R1(config)# **router ospf 1**

R1(config-router)# **area 0 authentication message-digest**

R2(config)# **router ospf 1**

R2(config-router)# **area 0 authentication message-digest**

R3(config)# **router ospf 1**

R3(config-router)# **area 0 authentication message-digest**

**Step 3: Configure the MD5 key for all the routers in area 0.**

Configure an MD5 key on the serial interfaces on **R1**, **R2** and **R3**. Use the password **MD5pa55** for key **1**.

R1(config)# **interface s0/0/0**

R1(config-if)# **ip ospf message-digest-key 1 md5 MD5pa55**

R2(config)# **interface s0/0/0**

R2(config-if)# **ip ospf message-digest-key 1 md5 MD5pa55**

R2(config-if)# **interface s0/0/1**

R2(config-if)# **ipospf message-digest-key 1 md5 MD5pa55**

R3(config)# **interface s0/0/1**

R3(config-if)# **ipospf message-digest-key 1 md5 MD5pa55**

**Step 4: Verify configurations.**

1. Verify the MD5 authentication configurations using the commands **show ipospf interface**.
2. Verify end-to-end connectivity by pinging R1 from R3

**Part 2: Configure NTP**

**Step 1: Enable NTP authentication on PC-A.**

1. On **PC-A**, click **NTP** under the Services tab to verify NTP service is enabled.
2. To configure NTP authentication, click **Enable** under Authentication. Use key **1** and password **NTPpa55**

**Experiment No: Class: TYIT**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** for authentication.

**Step 2: Configure R1, R2, and R3 as NTP clients.**

R1(config)# **ntp server 192.168.1.5**

R2(config)# **ntp server 192.168.1.5**

R3(config)# **ntp server 192.168.1.5**

Verify client configuration using the command **show ntp status**.

**Step 3: Configure routers to update hardware clock.**

Configure **R1**, **R2**, **and R3** to periodically update the hardware clock with the time learned from NTP.

R1(config)# **ntp update-calendar**

R2(config)# **ntp update-calendar**

R3(config)# **ntp update-calendar**

Exit global configuration and verify that the hardware clock was updated using the command **show clock**.

**Part 3: Configure Routers to Log Messages to the Syslog Server**

**Step 1: Configure the routers to identify the remote host (Syslog Server) that will receive logging messages.**

R1(config)# **logging host 192.168.1.6**

R2(config)# **logging host 192.168.1.6**

R3(config)# **logging host 192.168.1.6**

The router console will display a message that logging has started.

**Step 2: Verify logging configuration.**

Use the command **show logging** to verify logging has been enabled.

**Step 3: Examine logs of the Syslog Server.**

From the **Services** tab of the **Syslog Server**’s dialogue box, select the **Syslog** services button. Observe the logging messages received from the routers.

**Note**: Log messages can be generated on the server by executing commands on the router. For example, entering and exiting global configuration mode will generate an informational configuration message. You may need to click a different service and then click **Syslog** again to refresh the message display.

**Part 4: Configure R3 to Support SSH Connections**

**Step 1: Configure a domain name.**

**Experiment No: Class: TYIT**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** Configure a domain name of **sksecurity.com** on **R3**.

R3(config)# **ip domain-name sksecurity.com**

**Step 2: Configure users for login to the SSH server on R3.**

Create a user ID of **SSHadmin** with the highest possible privilege level and a secret password of **sksshpa55**.

R3(config)# **username SSHadmin privilege 15 secret sksshpa55**

**Step 3: Configure the incoming vty lines on R3.**

Use the local user accounts for mandatory login and validation. Accept only SSH connections.

R3(config)# **line vty 0 4**

R3(config-line)# **login local**

R3(config-line)# **transport input ssh**

**Step 4: Erase existing key pairs on R3.**

Any existing RSA key pairs should be erased on the router.

R3(config)# **crypto key zeroize rsa**

**Note**: If no keys exist, you might receive this message: % No Signature RSA Keys found in configuration.

**Step 5: Generate the RSA encryption key pair for R3.**

The router uses the RSA key pair for authentication and encryption of transmitted SSH data. Configure the RSA keys with a modulus of **1024**. The default is 512, and the range is from 360 to 2048.

R3(config)# **crypto key generate rsa**

The name for the keys will be: R3.sksecurity.com

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

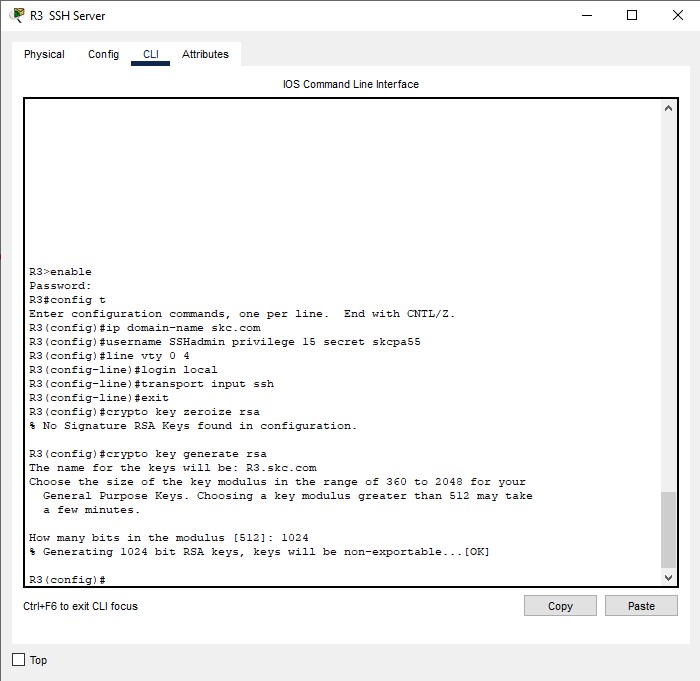
How many bits in the modulus [512]: **1024**

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

**Note**: The command to generate RSA encryption key pairs for **R3** in Packet Tracer differs from those used in the lab.

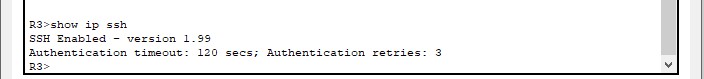
**Experiment No: Class: TYIT**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**



**Step 6: Verify the SSH configuration.**

Use the **show ip ssh** command to see the current settings. Verify that the authentication timeout and retries are at their default values of 120 and 3.



**Step 8: Attempt to connect to R3 via Telnet from PC-C.**

Open the Desktop of **PC-C**. Select the Command Prompt icon. From **PC-C**, enter the command to connect to **R3** via Telnet.

PC>**telnet 192.168.3.1**

This connection should fail because **R3** has been configured to accept only SSH connections on the virtual terminal lines.

**Experiment No: Class: TYIT**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Step 9: Connect to R3 using SSH on PC-C.**

Open the Desktop of **PC-C**. Select the Command Prompt icon. From **PC-C**, enter the command to connect to R3 via SSH. When prompted for the password, enter the password configured for the administrator sk**sshpa55**. PC>**ssh –l SSHadmin 192.168.3.1**

**Step 10: Connect to R3 using SSH on R2.**

To troubleshoot and maintain **R3**, the administrator at the ISP must use SSH to access the router CLI. From the CLI of **R2**, enter the command to connect to **R3** via SSH version **2** using the **SSHadmin** user account.

When prompted for the password, enter the password configured for the administrator: **sksshpa55**. R2# **ssh –v 2 –l SSHadmin 10.2.2.1**

**Step 11: Check results.**

Your completion percentage should be 100%. Click **Check Results** to view the feedback and verification of which required components have been completed.

