Lab 03

Configure Cisco Routers for Syslog, NTP, and SSH Operations

Name: Syed Asghar Abbas Zaidi	**Student ID: 07201**

2.1 Objective

The Objectives of this lab are:

- Configure OSPF MD5 authentication.
- Configure NTP.
- Configure routers to log messages to the syslog server.
- Configure R3 to support SSH connections.

2.2 Introduction

In this lab, you will configure OSPF MD5 authentication for secure routing updates

The NTP Server is the master NTP server in this lab. You will configure authentication on the NTP server and the routers. You will configure the routers to allow the software clock to be synchronized by NTP to the time server. Also, you will configure the routers to periodically update the hardware clock with the time learned from NTP.

The Syslog Server will provide message logging in this lab
. You will configure the routers to identify the remote host (Syslog server) that will receive logging messages.

You will need to configure timestamp service for logging on the routers. Displaying the correct time and date in Syslog messages is vital when using Syslog to monitor a network.

You will configure R3 to be managed securely using SSH instead of Telnet. The servers have been pre-configured for NTP and Syslog services respectively. NTP will not require authentication. The routers have been pre-configured with the following passwords:

Enable password: **ciscoenpa55**
Password for vty lines: **ciscovtypa55**

Note: Note: MD5 is the strongest encryption supported in the version of Packet Tracer used to develop this lab. Although MD5 has known vulnerabilities, you should use the encryption that meets the security requirements of your organization. In this lab, the security requirement specifies MD5.

Topology

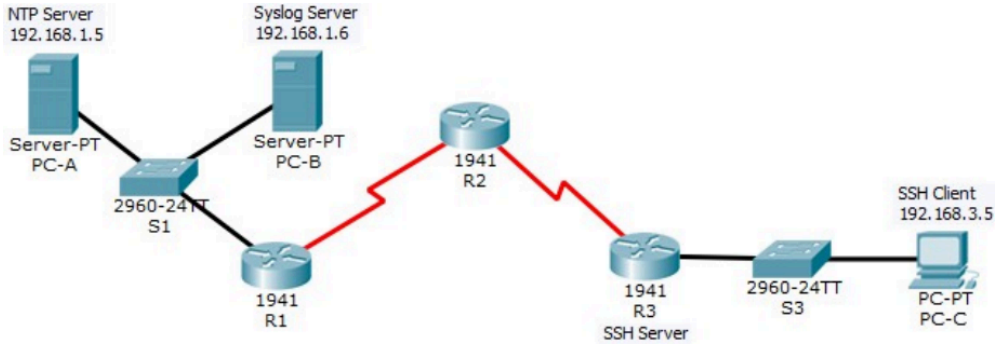


Figure 1: Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.5	255.255.255.0	192.168.1.1	S1 F0/6
PC-B	NIC	192.168.1.6	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	192.168.3.5	255.255.255.0	192.168.3.1	S3 F0/18

Table 1: Addressing Table

Task 1: Configure OSPF MD5 Authentication

1. Construct the topology as shown in Figure 1. Provide addresses to all devices using the values given in Table 1. Test connectivity. All devices should be able to ping all other IP addresses.

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

```
R1(config)# router ospf 1
R1(config-router)# area 0 authentication message-digest
```

Router 1:

```
R1(config)#router ospf 1
R1(config-router)#area 0 authentication message-digest
```

Router 2:

```
R2(config)#router ospf 1
R2(config-router)#area 0 authentication message-digest
```

Router 3:

```
R2(config)#router ospf 1
R2(config-router)#area 0 authentication message-digest
```

3. Configure the MD5 key for all the routers in area 0. Use the password **MD5pa55** for key

```
R1(config)# interface s0/0/0
R1(config-if)# ip ospf message-digest-key 1 md5 MD5pa55
```

Router 1:

```
R1(config-router)#interface s0/0/0
R1(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
```

Router 2:

```
R2(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
R2(config-if)#interface s0/0/1
```

Router 3:

```
R3(config-router)#interface s0/0/1

R3(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
```

4. Verify configurations.
   a. Verify the MD5 authentication configurations using the commands **show ip ospf interface**.

b. Verify end-to-end connectivity.

Router 1:

```
R1#show ip ospf interface

GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.1.1, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
      No key configured, using default key id 0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30, Area 0
  Process ID 1, Router ID 192.168.1.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.2.2
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

Router 2:

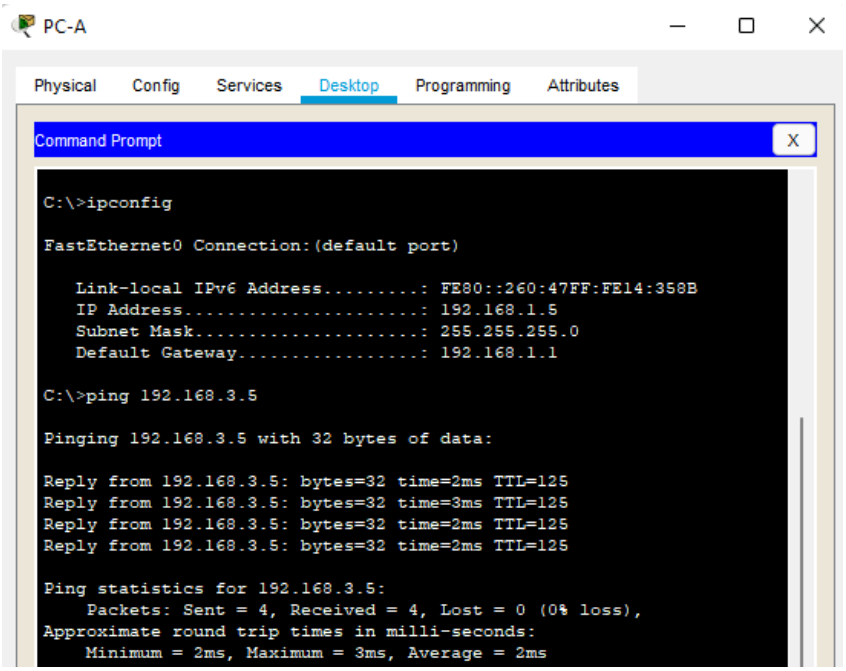
```
R2#show ip ospf interface

Serial0/0/1 is up, line protocol is up
  Internet address is 10.2.2.2/30, Area 0
  Process ID 1, Router ID 10.2.2.2, Network Type POINT-TO-POINT,
Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
5
    Hello due in 00:00:06
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.3.1
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.2/30, Area 0
  Process ID 1, Router ID 10.2.2.2, Network Type POINT-TO-POINT,
Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
5
    Hello due in 00:00:04
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.1.1
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

Router 3:

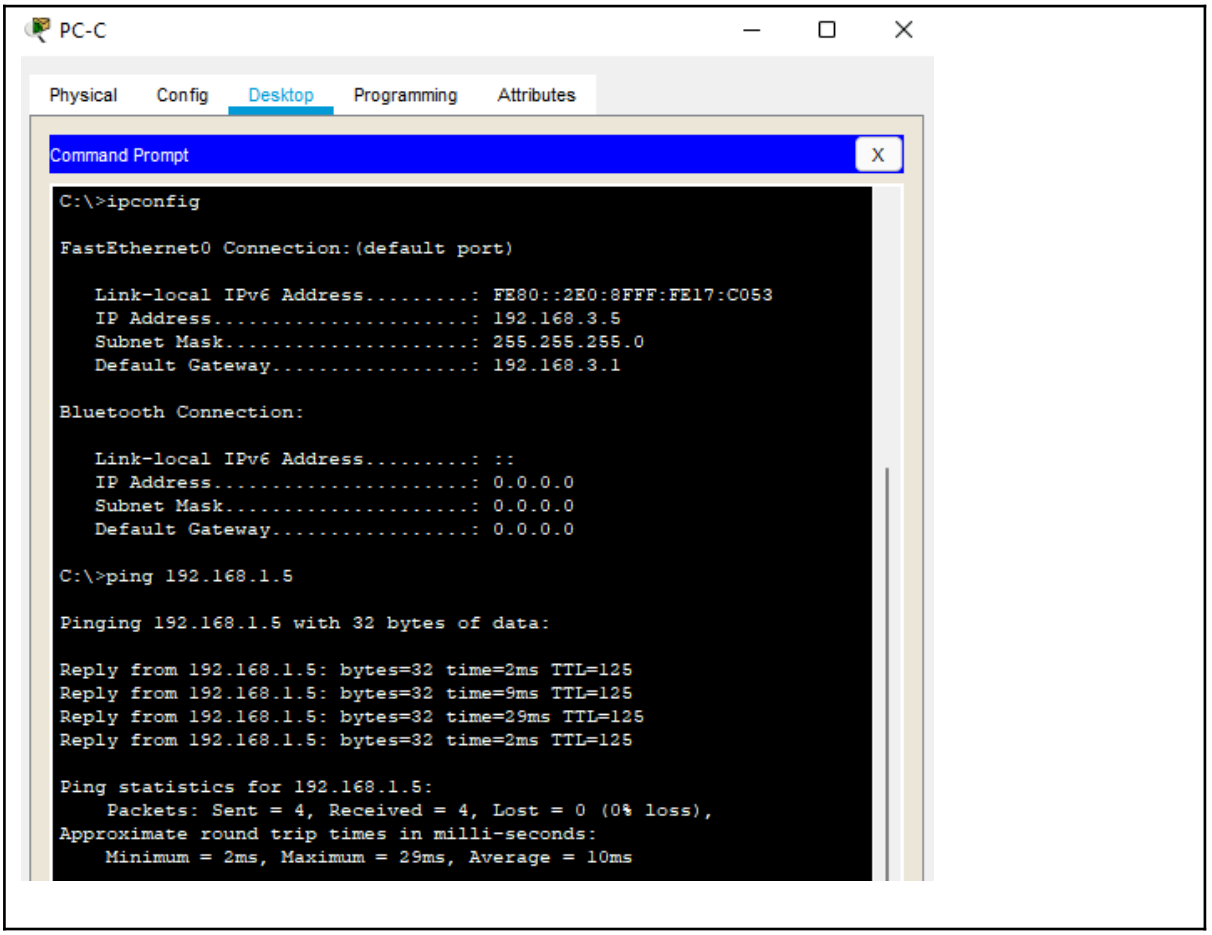
```
R3#show ip ospf interface

GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.3.1/24, Area 0
  Process ID 1, Router ID 192.168.3.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.3.1, Interface address 192.168.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
      No key configured, using default key id 0
Serial0/0/1 is up, line protocol is up
  Internet address is 10.2.2.1/30, Area 0
  Process ID 1, Router ID 192.168.3.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.2.2
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

Verifying connectivity:

PC-A to PC-C

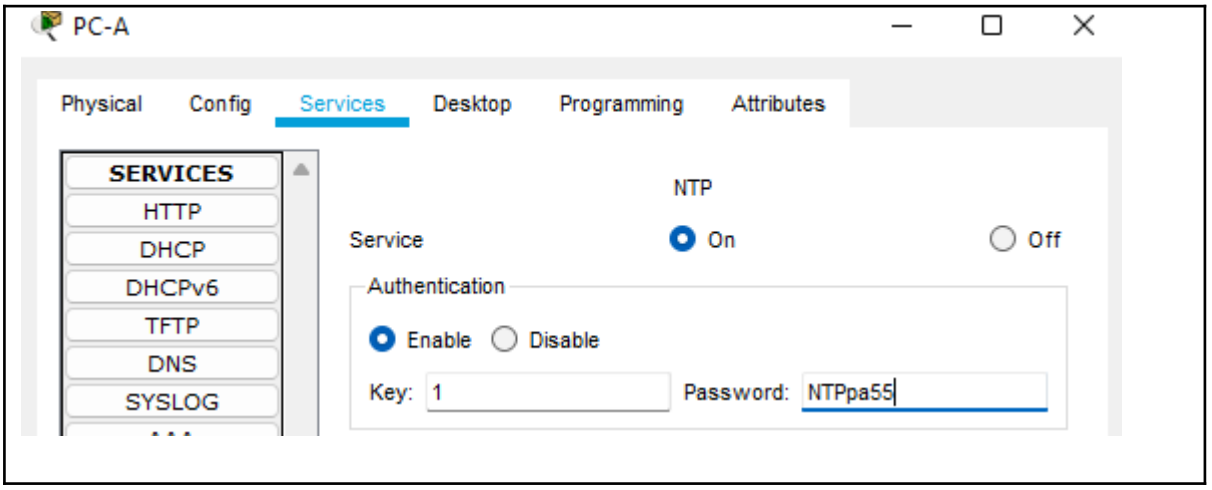


From PC-C to PC-A:



Task 2: Configure NTP

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



2) Configure R1, R2, and R3 as NTP clients. Verify client configuration using the command **show ntp status. Hint:** Use the **ntp server** command**.**

Router 1:

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

```
R1#show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is
2**24
reference time is 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1990)
clock offset is 0.00 msec, root delay is 0.00  msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec.
loopfilter state is 'FSET' (Drift set from file), drift is -
0.000001193 s/s system poll interval is 4, never updated.
```

Router 2:

```
R2#show ntp status
%NTP is not enabled.
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ntp server 192.168.1.5
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is
2**24
reference time is 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1990)
clock offset is 0.00 msec, root delay is 0.00  msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec.
loopfilter state is 'FSET' (Drift set from file), drift is -
0.000001193 s/s system poll interval is 4, never updated.
```

Router 3:

```
R3#show ntp status
%NTP is not enabled.
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ntp server 192.168.1.5
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is
2**24
reference time is 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1990)
clock offset is 0.00 msec, root delay is 0.00  msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec.
loopfilter state is 'FSET' (Drift set from file), drift is -
0.000001193 s/s system poll interval is 4, never updated.
```

3) Configure routers to update hardware clock. **Hint:** use the **ntp update-calendar** command**.**

Router 1, 2 and 3 respective:

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ntp update-calendar

R2(config)#ntp update-calendar

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

4) Configure NTP authentication on **R1**, **R2**, and **R3** using key **1** and password **NTPpa55.**

- R1(config)# **ntp authenticate**
- R1(config)# **ntp trusted-key 1**
- R1(config)# **ntp authentication-key 1 md5 NTPpa55**

Router 1,2,3 respective:

```
R1(config)#ntp authenticate
R1(config)#ntp trusted-key 1
R1(config)#ntp authentication-key 1 md5 NTPpa55

R2(config)#ntp authenticate
R2(config)#ntp trusted-key 1
R2(config)#ntp authentication-key 1 md5 NTPpa55
```

```
R3(config)#ntp authenticate
R3(config)#ntp trusted-key 1
R3(config)#ntp authentication-key 1 md5 NTPpa55
```

5) Configure routers to timestamp log messages.

```
R1(config)# service timestamps log datetime msec
```

Router 1,2,3 respectively:

```
R1(config)#service timestamps log datetime msec
R2(config)#service timestamps log datetime msec
R3(config)#service timestamps log datetime msec
```

Task 3: Configure Routers to Log Messages to the Syslog Server

1. Configure the routers to identify the remote host (Syslog Server) that will receive logging messages. On PC-A, click NTP under the Services tab to verify NTP service is enabled. **Hint:** use the **logging host** command.
   The router console will display a message that logging has started.

Router 1,2,3 respectively:

```
R1(config)#logging host 192.168.1.6
R2(config)#logging host 192.168.1.6
R3(config)#logging host 192.168.1.6
```

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

Router 1:

```
R1# show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
          0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.


No Inactive Message Discriminator.


    Console logging: level debugging, 14 messages logged, xml
disabled,
          filtering disabled
    Monitor logging: level debugging, 14 messages logged, xml
disabled,
          filtering disabled
    Buffer logging:  disabled, xml disabled,
          filtering disabled

    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped
    Trap logging: level informational, 14 message lines logged
        Logging to 192.168.1.6  (udp port 514,  audit disabled,
              authentication disabled, encryption disabled, link up),
              2 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
```

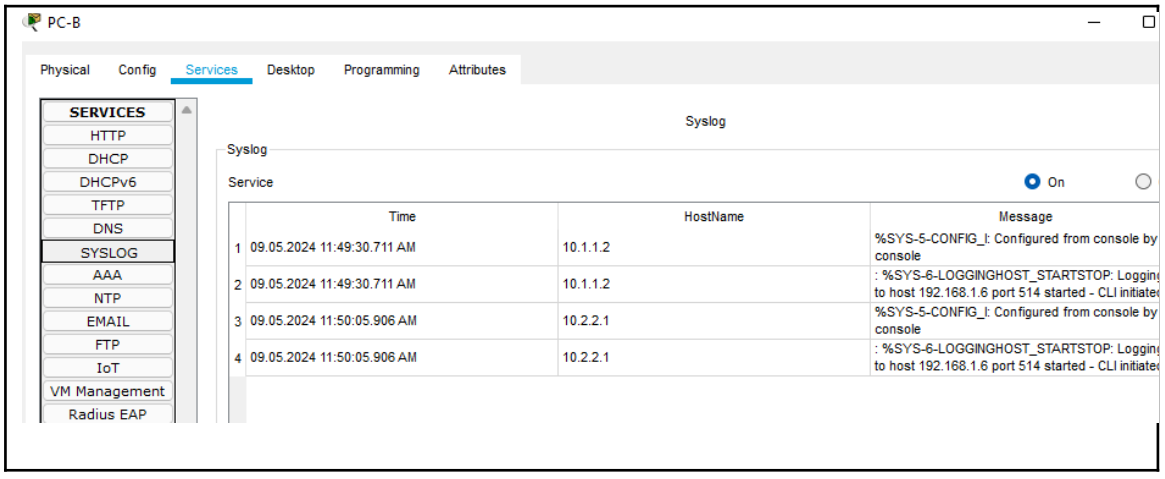
Router 2:

```
R2#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
          0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.


No Inactive Message Discriminator.


    Console logging: level debugging, 22 messages logged, xml disabled,
          filtering disabled
    Monitor logging: level debugging, 22 messages logged, xml disabled,
          filtering disabled
    Buffer logging:  disabled, xml disabled,
          filtering disabled

    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped
    Trap logging: level informational, 22 message lines logged
        Logging to 192.168.1.6  (udp port 514,  audit disabled,
              authentication disabled, encryption disabled, link up),
              2 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
```

Router 3:

```
R3#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
          0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.


No Inactive Message Discriminator.


    Console logging: level debugging, 14 messages logged, xml disabled,
          filtering disabled
    Monitor logging: level debugging, 14 messages logged, xml disabled,
          filtering disabled
    Buffer logging:  disabled, xml disabled,
          filtering disabled

    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped
    Trap logging: level informational, 14 message lines logged
        Logging to 192.168.1.6  (udp port 514,  audit disabled,
              authentication disabled, encryption disabled, link up),
              2 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
```

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.



Task 4: Configure R3 to Support SSH Connections

1. Configure a domain name of **ccnasecurity.com** on R3.

```
R3(config)#ip domain-name ccnasecurity.com
R3(config)#end
R3#
*Sep 05, 11:53:02.5353: SYS-5-CONFIG_I: Configured from console by
console
R3#show running-config | include ip domain-name
ip domain-name ccnasecurity.com
```

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 **ciscosshpa55.**

   `R3(config)#` **`username SSHadmin privilege 15 secret ciscosshpa55`**

```
R3(config)#username SSHadmin privilege 15 secret ciscosshpa55
```

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
```

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.

```
R3(config)#crypto key zeroize rsa
% No Signature RSA Keys found in configuration.
```

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
```

```
R3(config)# crypto key generate rsa
The name for the keys will be: R3.ccnasecurity.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]
```

Proof of me doing it:

```
R3(config)#crypto key generate rsa
The name for the keys will be: R3.ccnasecurity.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]
```

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.

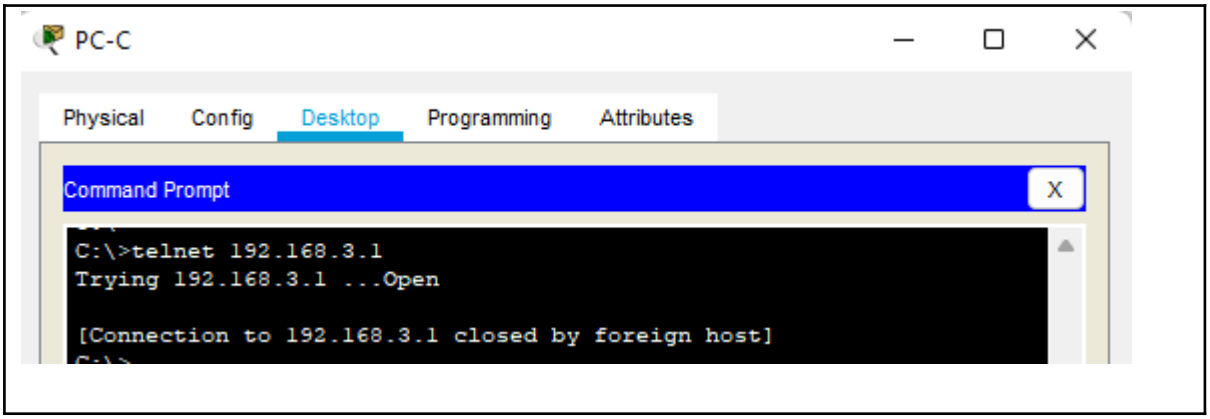
```
R3#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
```

7. Configure SSH timeouts and authentication parameters. The default SSH timeouts and authentication parameters can be altered to be more restrictive. Set the timeout to **90** seconds, the number of authentication retries to **2**, and the version to **2**. Issue the **show ip ssh** command again to confirm that the values have been changed.

```
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip ssh time-out 90
R3(config)#ip ssh authentication-retries 2
R3(config)#ip ssh version 2
R3(config)#end
```

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.

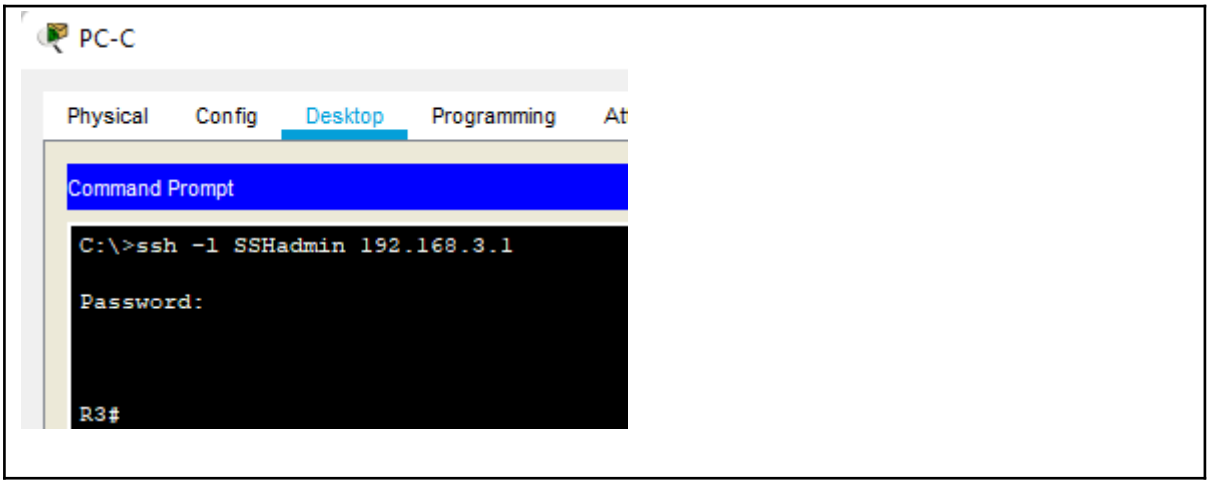
   PC> **telnet 192.168.3.1**



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

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 **ciscosshpa55**.\

   PC> **ssh -l SSHadmin 192.168.3.1**



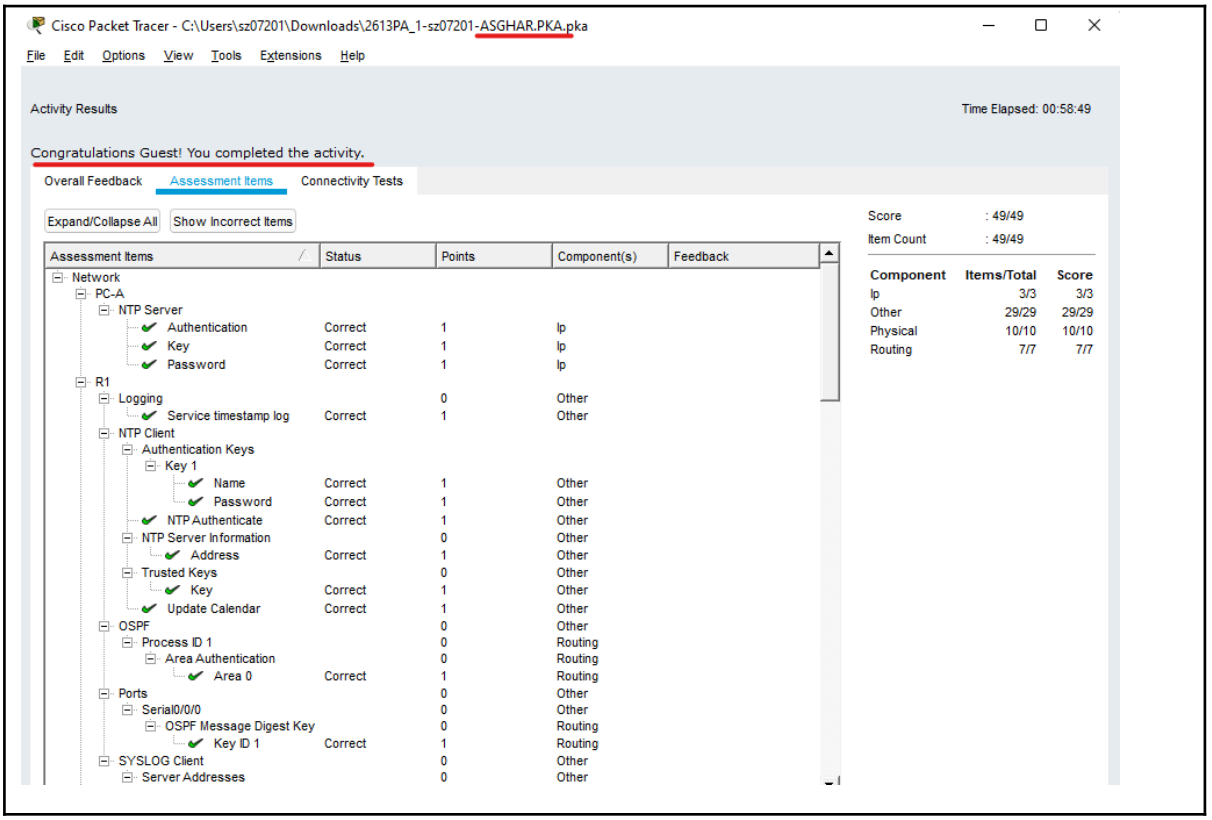
10. Connect to R3 using SSH on R2. To troubleshoot and maintain R3, the administrator at the ISP must use SSH to access the router CLI. From the CLI of **R2,** enter the command to connect to **R3** via SSH version **2** using the **SSHadmin** user account. When prompted for the password, enter the password configured for the administrator: **ciscosshpa55**.

    `R2# ssh -v 2 -l SSHadmin 10.2.2.1`

```
R2>en
Password:
R2#ssh -v 2 -l SSHadmin 10.2.2.1

Password:



R3#
```

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

Proof of completion of Lab:


Cisco Packet Tracer - C:\Users\sz07201\Downloads\2613PA_1-sz07201-ASGHAR.PKA.pka
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 00:58:49
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Show Incorrect Items
Assessment Items
Status
Points
Component(s)
Feedback
Network
PC-A
NTP Server
Authentication Correct 1 Ip
Key Correct 1 Ip
Password Correct 1 Ip
R1
Logging 0 Other
Service timestamp log Correct 1 Other
NTP Client
Authentication Keys
Key 1
Name Correct 1 Other
Password Correct 1 Other
NTP Authenticate Correct 1 Other
NTP Server Information 0 Other
Address Correct 1 Other
Trusted Keys 0 Other
Key Correct 1 Other
Update Calendar Correct 1 Other
OSPF 0 Other
Process ID 1 0 Routing
Area Authentication 0 Routing
Area 0 Correct 1 Routing
Ports 0 Other
Serial0/0/0 0 Other
OSPF Message Digest Key 0 Routing
Key ID 1 Correct 1 Routing
SYSLOG Client 0 Other
Server Addresses 0 Other
Score : 49/49
Item Count : 49/49
Component Items/Total Score
Ip 3/3 3/3
Other 29/29 29/29
Physical 10/10 10/10
Routing 7/7 7/7

✔ Address	Correct	1	Other
R2			
Logging		0	Other
✔ Service timestamp log	Correct	1	Other
NTP Client			
Authentication Keys			
Key 1			
✔ Name	Correct	1	Other
✔ Password	Correct	1	Other
✔ NTP Authenticate	Correct	1	Other
NTP Server Information		0	Other
✔ Address	Correct	1	Other
Trusted Keys		0	Other
✔ Key	Correct	1	Other
✔ Update Calendar	Correct	1	Other
OSPF		0	Other
Process ID 1		0	Routing
Area Authentication		0	Routing
✔ Area 0	Correct	1	Routing
Ports			
Serial0/0/0		0	Other
OSPF Message Digest Key		0	Routing
✔ Key ID 1	Correct	1	Routing
Serial0/0/1		0	Other
OSPF Message Digest Key		0	Routing
✔ Key ID 1	Correct	1	Routing
SYSLOG Client		0	Other
Server Addresses		0	Other
✔ Address	Correct	1	Other
R3			
✔ IP Domain Name	Correct	1	Other
Logging		0	Other
✔ Service timestamp log	Correct	1	Other
NTP Client			
Authentication Keys			
Key 1			
✔ Name	Correct	1	Other
✔ Password	Correct	1	Other
✔ NTP Authenticate	Correct	1	Other
NTP Server Information		0	Other
✔ Address	Correct	1	Other
Trusted Keys		0	Other
✔ Key	Correct	1	Other
✔ Update Calendar	Correct	1	Other
OSPF		0	Other
Process ID 1		0	Routing
Area Authentication		0	Routing
✔ Area 0	Correct	1	Routing
Ports		0	Other
Serial0/0/1		0	Other
OSPF Message Digest Key		0	Routing

Key ID 1	Correct	1	Routing
SSH Server			
SSH Authentication Retries	Correct	1	Other
SSH Timeout	Correct	1	Other
SSH Version	Correct	1	Other
SYSLOG Client		0	Other
Server Addresses		0	Other
Address	Correct	1	Other
User Names		0	Other
Username	Correct	1	Other
VTY Lines			
VTY Line 0			
Login	Correct	1	Physical
Transport Input	Correct	1	Physical
VTY Line 1			
Login	Correct	1	Physical
Transport Input	Correct	1	Physical
VTY Line 2			
Login	Correct	1	Physical
Transport Input	Correct	1	Physical
VTY Line 3			
Login	Correct	1	Physical
Transport Input	Correct	1	Physical
VTY Line 4			
Login	Correct	1	Physical
Transport Input	Correct	1	Physical

Assessment Rubric

Lab 03

Configure Cisco Routers for Syslog, NTP and SSH Operations

Name: Syed Asghar Abbas Zaidi	**Student ID: 07201**

Points Distribution

Task No.	**LR 2 Simulation**	**LR9 Report**
Task 1	20	
Task 2	20	
Task 3	10	
Task 4	30	
Total	/80	/10
CLO Mapped	CLO 1	CLO1

Affective Domain Rubric		**Points**	**CLO Mapped**
AR 7	Report Submission	/10	CLO 1

CLO	**Total Points**	**Points Obtained**
1	100	
Total	**100**	

For description of different levels of the mapped rubrics, please refer the provided Lab Evaluation Assessment Rubrics and Affective Domain Assessment Rubrics.

Lab Evaluation Assessment Rubric

#	Assessment Elements	Level 1: Unsatisfactory Points 0-1	Level 2: Developing Points 2	Level 3:Good Points 3	Level 4:Exemplary Points 4
LR2	**Program/Code / Simulation Model/ Network Model**	Program/code/simulation model/network model does not implement the required functionality and has several errors. The student is not able to utilize even the basic tools of the software.	Program/code/simulation model/network model has some errors and does not produce completely accurate results. Student has limited command on the basic tools of the software.	Program/code/simulation model/network model gives correct output but not efficiently implemented or implemented by computationally complex routine.	Program/code/simulation /network model is efficiently implemented and gives correct output. Student has full command on the basic tools of the software.
LR9	**Report**	All the in-lab tasks are not included in report and / or the report is submitted too late.	Most of the tasks are included in report but are not well explained. All the necessary figures / plots are not included. Report is submitted after due date.	Good summary of most the in-lab tasks is included in report. The work is supported by figures and plots with explanations. The report is submitted timely.	Detailed summary of the in-lab tasks is provided. All tasks are included and explained well. Data is presented clearly including all the necessary figures, plots and tables.