Practical 1: Packet Tracer - Configure Cisco Routers for Syslog, NTP, and SSH Operations

IP Address Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Gig0/0	192.168.1.1	255.255.255.0	-
	Se0/1/0	10.1.1.1	255.255.255.252	-
R2	Se0/1/0	10.1.1.2	255.255.255.252	-
	Se0/1/1	10.2.2.2	255.255.255.252	-
R3	Gig0/0	192.168.3.1	255.255.255.0	-
	Se0/1/0	10.2.2.1	255.255.255.252	-
S1	Fa0	192.168.1.5	255.255.255.0	192.168.1.1
S2	Fa0	192.168.1.6	255.255.255.0	192.168.1.1
PC	Fa0	192.168.3.5	255.255.255.0	192.168.3.1

OSPF Routing:

1. R1

R1(config)#router ospf 1

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

R1(config-router)#network 10.1.1.2 0.255.255.255 area 0

R1(config-router)#exit

2. R2

R2(config)#router ospf 1

R2(config-router)#network 10.1.1.1 0.255.255.255 area 0

R2(config-router)#network 10.2.2.1 0.255.255.255 area 0

R2(config-router)#exit

3. R3

R3(config)#router ospf 1

R3(config-router)#network 192.168.3.1 0.0.0.255 area 0

R3(config-router)#network 10.2.2.2 0.255.255.255 area 0

R3(config-router)#exit

a. Configure OSPF MD5 Authentication:

1. Test Connectivity.

2. Configure OSPF MD5 Authentication

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

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

R3(config)#router ospf 1
R3(config-router)#area 0 authentication message-digest
R3(config-router)#exit
```

3. Configure MD5 for all keys

```
R1(config)#int Se0/1/0
R1(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
R1(config-if)#exit

R2(config)#int Se0/1/0
R2(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
R2(config-if)#exit
R2(config)#int Se0/1/1
R2(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
R2(config-if)#exit

R3(config)#int Se0/1/0
R3(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
R3(config-if)#exit
```

b. Configure NTP

1. In S1, under Services tab make NTP server on and Enable Authentication. Enter key **1** and password **NTPpa55.**

2. Configure Routers 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
```

3. Configure router to update hardware clocks

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

R2(config)#ntp update-calendar

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

4. Configure NTP authentication on routers

```
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

R2(config)#service timestamps log datetime msec

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

c. Configure routers to log messages to syslog server (i.e., S2)

1. Configure routers for logging

```
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 log message

In config prompts of all router type exit two times and enable it router again. After this go to S2 Services tab and under syslog you will see log messages.

d. Configure R3 to support SSH messages

```
R3(config)#ip domain-name tyit.com

R3(config)#username SSHadmin privilege 15 secret 45it

R3(config)#line vty 0 4

R3(config-line)#login local

R3(config-line)#transport input ssh

R3(config-line)#exit

R3(config)#crypto key zeroize rsa

R3(config)#crypto key generate rsa

How many bits in the modulus [512]: 1024

R3(config)#ip ssh time-out 90

R3(config)#ip ssh authentication-retries 2

R3(config)#ip ssh version 2
```

On PC, open command prompt and type

```
C:\ telnet 192.168.3.1
```

This connection should fail

Then, on PC's command prompt type

```
C:\ ssh -l SSHadmin 192.168.3.1
```

Enter the password as 45it and you connection should be successful and it should display R3 prompt.

Connect to R3 using SSH in R2, go to R2 and type

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

And enter password as 45it and you should be able to see R3# after entering

If YES, Practical Successful

If NO, Try Again