Practical 1

Configure Routers for Syslog, NTP and SSH Operations - Packet Tracer

Addressing Table

Device	Interface	IP Addresses	Subnet Masks	Default Gateway	Switch Port
R1	G 0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S 0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
R2	S 0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S 0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
R3	G 0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S 0/0/1	10.22.1	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

Step 1: Test Connectivity

```
PC> ping 192.168.3.5
PC> ping 192.168.1.5
```

Step 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

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

```
R3 (config) # router ospf 1
R3 (config-router)# area0 authentication message-digest

R1 (config)# interface S 0/0/0
R1(config-if)#ip ospf message-digest-key 1 md5
MD5pass

R2 (config) # interface S0/0/0
R2 (config-if) # ip ospf message-digest-key-1 md5
MD5pass
R2 (config-if) # interface S0/0/1
R2 (config-if) # ip ospf message-digest-key 1 md5
MD5pass

R3(config) #interface S0/0/1
R3(config-if) #ip ospf message-digest-key 1md5
MD5pass
```

Step 4 : Verify Configurations

```
R1# sh ip ospf interface.
```

6] Configure NTP

Step1: Enable NTP authentication on PC-A

ⓐ On PCA, click NTP under the services tab to verify NTP service is enabled.

ⓑ To configure NTP authentication, click enable under Authenication. use Key 1 and password NTP pass for authentication.

Step 2: Configure R1, R2, 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
```

```
R1 # sh ntp status
```

Step 3: Configure routers to update hardware clock

```
R1 (config) # ntp update-calendar
R2 (config) # ntp update-calendar
R3 (config) # ntp update- ~~calendar~~ calendar
R3 (config) # exit
R3 # show clock
```

Step 4: Configure NTP authentication on the routers

```
R1 (config) # ntp authenticate
R1 (config) # ntp trusted-key 1
R1. (config) # ntp authentication-key 1 md5 NTP pass.
```

```
R2 (config) # ntp authenticate
R2 (config) # ntp trusted-Key-1
R2 (config) # ntp authentication-Key1 md5 NTPpass
```

Step 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
```

```
R1 # show ntp status.
```

1.c] 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
```

Step 2: Verify logging configurations.

```
R1 # show logging
```

Step 3: Examine logs of the syslog server

From the services tab of the syslog services dialogue box, select the syslog services button, Observe the logging messages received from the routers.

Configure R3 to support SSH connections

Step1: Configure a domain name. Configure a domain name of ccnasecurity.com on R3

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

Step 2: configure users for login to SSH server on R3

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

Step 3: Configure the incoming vty lines on R3

```
R3 (config)# line vty 0 4
R3 (config-line)# login local
R3 (config-line)# transport input ssh
```

Step 4: Erase existing key pairs 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

```
R3(config)# crypto key generate rsa.
```

Step 6: Verify the SSH configuration

```
R3 # show ip SSH
```

Step 7: configure SSH timeouts and authentication parameters.

```
R3 (config) # ip ssh time-out 90
R3 (config) # ip ssh authentication -retries 2
R3 (config) # ip ssh version 2
```

```
R3 # show ip ssh
```

Step 8 - Attempt to connect to R3 via telnet from PC-C

```
PC > telnet 192.168.3.1
```

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

Step 9: Connect to R3 using SSH on PC-C

```
PC > ssh -l SSHadmin 192.168.3.1
    password - MyPass
```

Step 10: Connect R3 using SSH on R2

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