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

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

1. Configure the MD5 key for all the routers in area 0.

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)# ip ospf message-digest-key 1 md5 MD5pa55

R3(config)# interface s0/0/1

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

1. Verify configurations.

show ip ospf interface.

**Configure NTP**

1. Enable NTP authentication on PC-A.

On PC-A, click NTP under the Services tab to verify NTP service is enabled.

To configure NTP authentication, click Enable under Authentication. Use key 1 and password NTPpa55 for authentication.

1. 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.

1. Configure routers to update hardware clock. Configure R1, R2, and R3 to periodically

R1(config)# ntp update-calendar

R2(config)# ntp update-calendar

R3(config)# ntp update-calendar

1. Configure NTP authentication on the 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

1. 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

**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.

R1(config)# logging host 192.168.1.6

R2(config)# logging host 192.168.1.6

R3(config)# logging host 192.168.1.6

1. Verify logging configuration.

show logging to verify logging has been enabled.

1. 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.

**Configure R3 to Support SSH Connections**

1. Configure a domain name.

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

1. 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

1. Configure the incoming vty lines on R3.

R3(config)# line vty 0 4

R3(config-line)# login local

R3(config-line)# transport input ssh

1. Erase existing key pairs on R3.

R3(config)# crypto key zeroize rsa

1. Generate the RSA encryption key pair for R3.

R3(config)# crypto key generate rsa

1. Verify the SSH configuration.

show ip ssh

1. 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

show ip ssh

1. 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

1. 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

1. Connect to R3 using SSH on R2.

R2# ssh –v 2 –l SSHadmin 10.2.2.1