Run following commands on all routers

Enable secret tyit1819

Router ospf 1

area 0 authentication message-digest

exit

Configure message digest

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

**Configure Local AAA Authentication for Console Access on R**

1. Test connectivity PCA to PCB and PCC ,PCB to PCC
2. Configure a local username on R1.

R1(config)# **username Admin1 secret admin1pa55**

1. **Configure local AAA authentication for console access on R1.**

R1(config)# **aaa new-model**

R1(config)# **aaa authentication login default local**

1. **Configure the line console to use the defined AAA authentication method.**

R1(config)# **line console 0**

R1(config-line)# **login authentication default**

1. **Verify the AAA authentication method.**

R1(config-line)# end

%SYS-5-CONFIG\_I: Configured from console by console

R1# exit

**Configure Local AAA Authentication for vty Lines on R1**

1. **Configure domain name and crypto key for use with SSH.**

R1(config)# **ip domain-name ccnasecurity.com**

R1(config)# **crypto key generate rsa**

1. Configure a named list AAA authentication method for the vty lines on R1.

R1(config)# **aaa authentication login SSH-LOGIN local**

1. **Configure the vty lines to use the defined AAA authentication method.**

R1(config)# **line vty 0 4**

R1(config-line)# **login authentication SSH-LOGIN**

R1(config-line)# **transport input ssh** R1(config-line)# **end**

1. **Verify the AAA authentication method.**

PC-A..

PC> ssh –l Admin1 192.168.1.1