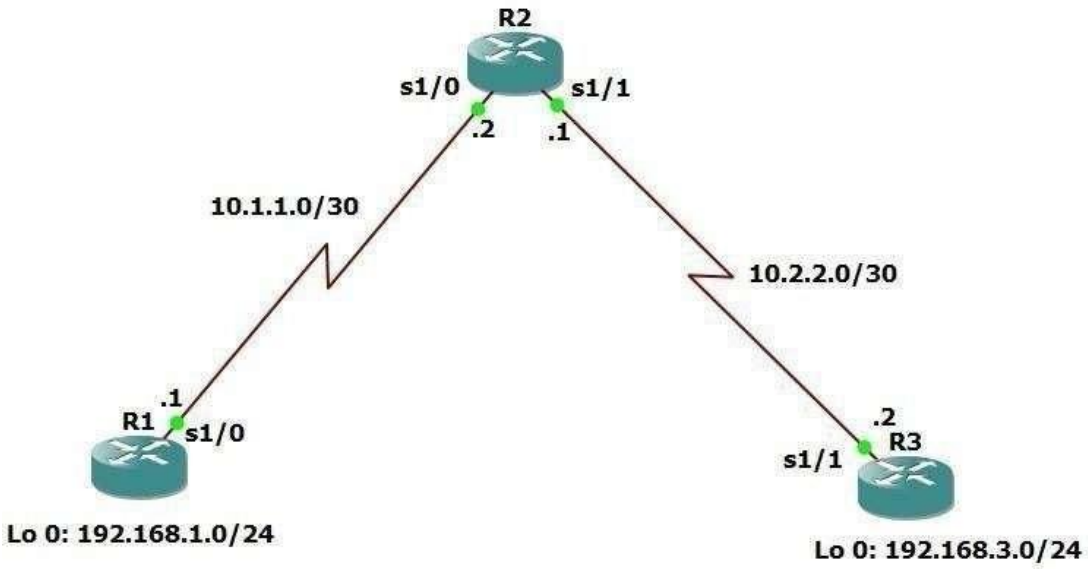
Practical :04

Aim: Configuring Secure Management Plane (On GNS3)



Step 1: Configure loopbacks and assign addresses.

```
R1#conf t
R1(config)#int lo 0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#int se1/0
R1(config-if)#ip add 10.1.1.1 255.255.255.252
R1(config-if)#no shut
R1(config-if)#exit

R2#conf t
R2(config)#int se1/0
R2(config-if)#ip add 10.1.1.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#int se1/1
R2(config-if)#ip add 10.2.2.1 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit

R3#conf t
R3(config)#int lo 0
R3(config-if)#ip add 192.168.3.1 255.255.255.0
R3(config-if)#exit
R3(config)#int se1/1
R3(config-if)#ip add 10.2.2.2 255.255.255.252
```

R3(config-if)#no shut
R3(config-if)#exit

Step 2: Configure static routes.
R1#conf t
R1(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2

R3#conf t
R3(config)#ip route 0.0.0.0 0.0.0.0 10.2.2.1

R2#conf t
R2(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.1
R2(config)#ip route 192.168.3.0 255.255.255.0 10.2.2.2

Verify connectivity from R1

```
R1#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms
R1#ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/64/76 ms
R1#ping 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/31/48 ms
R1#ping 10.2.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/27/32 ms
R1#ping 10.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/58/60 ms
R1#ping 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/56/64 ms
R1#
```

Step 3: Secure management access.

a. On R1, use the **security passwords** command to set a minimum password length of 10 characters.

R1(config)#security passwords min-length 10

b. Configure the enable secret encrypted password on both routers.

R1(config)#enable secret class12345

c. Configure a console password and enable login for routers. For additional security, the **exectimeout** command causes the line to log out after 5 minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry. **Note**: To avoid repetitive logins during this lab, the **exec-timeout** command can be set to 0 0, which prevents it from expiring.

```
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
```

d. Configure the password on the vty lines for router R1.

```
R1(config)#line vty 0 4
R1(config-line)#password ciscovtypass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#exit
```

e. The aux port is a legacy port used to manage a router remotely using a modem and is hardly ever used. Therefore, disable the aux port.

```
R1(config)#line aux 0
R1(config-line)#no exec
R1(config-line)#end
```

f. Use the **service password-encryption** command to encrypt the line console and vty passwords.

```
R1#conf t
R1(config)#service password-encryption
```

g. Configure a warning to unauthorized users with a message-of-the-day (MOTD) banner using the **banner motd** command. When a user connects to one of the routers, the MOTD banner appears before the login prompt. In this example, the dollar sign ($) is used to start and end the message.

```
R1(config)#banner motd $Unauthorized access strictly prohibited!$
R1(config)#exit
```

Repeat the configuration portion of steps 3a through 3g on router R3.

```
R3#conf t
R3(config)#security passwords min-length 10
R3(config)#enable secret class12345
R3(config)#line console 0
R3(config-line)#password ciscoconpass
```

```
R3(config-line)#exec-timeout 5 0
R3(config-line)#login
R3(config-line)#logging synchronous
R3(config-line)#exit

R3(config)#line vty 0 4
R3(config-line)#password ciscovtypass
R3(config-line)#exec-timeout 5 0
R3(config-line)#login
R3(config-line)#exit

R3(config)#line aux 0
R3(config-line)#no exec
R3(config-line)#end

R3#conf t
R3(config)#service password-encryption
R3(config)#banner motd $Unauthorized access strictly prohibited!$
R3(config)#exit
```

Step 4: Configure enhanced username password security.

a. To create local database entry encrypted to level 4 (SHA256), use the **username** *name* **secret** *password* global configuration command. In global configuration mode, enter the following command:

```
R1#conf t
R1(config)#username JR-ADMIN secret class12345
R1(config)#username ADMIN secret class54321
```

b. Set the console line to use the locally defined login accounts.

```
R1(config)#line console 0
R1(config-line)#login local
R1(config-line)#exit
```

c. Set the vty lines to use the locally defined login accounts.

```
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#end
R1#
```

d. Repeat the steps 4a to 4c on R3.

```
R3#conf t
R3(config)#username JR-ADMIN secret class12345
R3(config)#username ADMIN secret class54321
R3(config)#line console 0
```

R3(config-line)#login local
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#login local
R3(config-line)#end

e. To verify the configuration, telnet to R3 from R1 and login using the ADMIN local database account.

Step 5: Enabling AAA RADIUS Authentication with Local User for Backup.

a. Always have local database accounts created before enabling AAA. Since we created two local database accounts in the previous step, then we can proceed and enable AAA on R1. R1(config)#aaa new-model

b. Configure the specifics for the first RADIUS server located at 192.168.1.101. Use **RADIUS1-pa55w0rd** as the server password.

R1(config)#radius server RADIUS-1
R1(config-radius-server)#address ipv4 192.168.1.101
R1(config-radius-server)#key RADIUS-1-pa55w0rd
R1(config-radius-server)#exit

c. Configure the specifics for the second RADIUS server located at 192.168.1.102. Use **RADIUS-2-pa55w0rd** as the server password.

R1(config)#radius server RADIUS-2
R1(config-radius-server)#address ipv4 192.168.1.102
R1(config-radius-server)#key RADIUS-2-pa55w0rd
R1(config-radius-server)#exit

d. Assign both RADIUS servers to a server group. R1(config)#aaa group server radius RADIUS-GROUP

R1(config-sg-radius)#server name RADIUS-1
R1(config-sg-radius)#server name RADIUS-2
R1(config-sg-radius)#exit

e. Enable the default AAA authentication login to attempt to validate against the server group. If they are not available, then authentication should be validated against the local database..

R1(config)#aaa authentication login default group RADIUS-GROUP local

f. Enable the default AAA authentication Telnet login to attempt to validate against the server group. If they are not available, then authentication should be validated against a case sensitive local database.

```
R1(config)#aaa authentication login TELNET-LOGIN group RADIUS-GROUP local-case
```

g. Alter the VTY lines to use the TELNET-LOGIN AAA authentiaiton method.

```
R1(config)#line vty 0 4
R1(config-line)#login authentication TELNET-LOGIN
R1(config-line)#exit
R1(config)#
```

h. Repeat the steps 5a to 5g on R3.

```
R3#conf t
R3(config)#aaa new-model
R3(config)#radius server RADIUS-1
R3(config-radius-server)#address ipv4 192.168.1.101
R3(config-radius-server)#key RADIUS-1-pa55w0rd
R3(config-radius-server)#exit
R3(config)#radius server RADIUS-2
R3(config-radius-server)#address ipv4 192.168.1.102
R3(config-radius-server)#key RADIUS-2-pa55w0rd
R3(config-radius-server)#exit
R3(config)#aaa group server radius RADIUS-GROUP
R3(config-sg-radius)#server name RADIUS-1
R3(config-sg-radius)#server name RADIUS-2
R3(config-sg-radius)#exit
R3(config)#aaa authentication login default group RADIUS-GROUP local
R3(config)#aaa authentication login TELNET-LOGIN group RADIUS-GROUP local-case
R3(config)#line vty 0 4
R3(config-line)#login authentication TELNET-LOGIN
R3(config-line)#exit
R3(config)#
```

i. To verify the configuration, telnet to R3 from R1 and login using the ADMIN local database

```
R1#telnet 10.2.2.2
Trying 10.2.2.2 ... Open
Unauthorized access strictly prohibited!
User Access Verification

Username: admin
Password:

% Authentication failed
```

```
R1#telnet 10.2.2.2
Trying 10.2.2.2 ... Open
Unauthorized access strictly prohibited!

User Access Verification

Username: ADMIN
Password:

R3>
```

Note: The actual login time is longer since the RADIUS servers are not available.

Step 6: Enabling secure remote management using SSH.

a. SSH requires that a device name and a domain name be configured. Since the router already has a name assigned, configure the domain name.

```
R1#conf t
R1(config)#ip domain-name ccnasecurity.com
```

b. The router uses the RSA key pair for authentication and encryption of transmitted SSH data. Although optional it may be wise to erase any existing key pairs on the router.

```
R1(config)#crypto key zeroize rsa
% No Signature Keys found in configuration.
```

c. Generate the RSA encryption key pair for the router. Configure the RSA keys with **1024** for the number of modulus bits. The default is 512, and the range is from 360 to 2048.

```
R1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.ccnasecurity.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

R1(config)#
*Apr  9 18:21:15.683: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

d. Configure SSH version 2 on R1.

```
R1#conf t
R1(config)#ip ssh version 2
```

e. Configure the vty lines to use only SSH connections.

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

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

f. Verify the SSH configuration using the **show ip ssh** command.

```
R1#sh ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQCusWpZxSxci4AXX7csxYc5winMsKCEdmk1t+PuK2aU
30msvz62cjmENZXcg582wcW6MsqNqCmQxWXeQuwt672MWsZ9x+8EncVJsmbPKPzO4tioSi0IRbpicD7A
fUFtMiqzreuJ5U6Uhpo8b9EBFJqnczLJAkUMyzDRq8OcRgFOTw==
R1#
```

g. Repeat the steps 6a to 6f on R3.
R3#conf t
R3(config)#ip domain-name ccnasecurity.com
R3(config)#crypto key zeroize rsa
% No Signature Keys found in configuration.

R3(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R3.ccnasecurity.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

R3(config)#
*Apr 9 18:24:19.763: %SSH-5-ENABLED: SSH 1.99 has been enabled
R3(config)#ip ssh version 2
R3(config)#line vty 0 4
R3(config-line)#transport input ssh
R3(config-line)#end
R3#

```
R3#sh ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQCizxUKc0w5wB/m8wbM9o0m17xXFJagVcTOWkQY3bfQ
sKai44Y6J/6ycE7ZnwUjRUOvkNXrKFUcd0BBtugSesjAxUV3LRilMpQWttab/V3klGNsZ+KaEKd8z09d
uAuXH5s+fdoPGkoDzb/xlFxRpGnDf7XNs0MsHjrWj32dp1p0Yw==
R3#
```

h. Although a user can SSH from a host using the SSH option of TeraTerm of PuTTY, a routercan also SSH to another SSH enabled device. SSH to R3 from R1