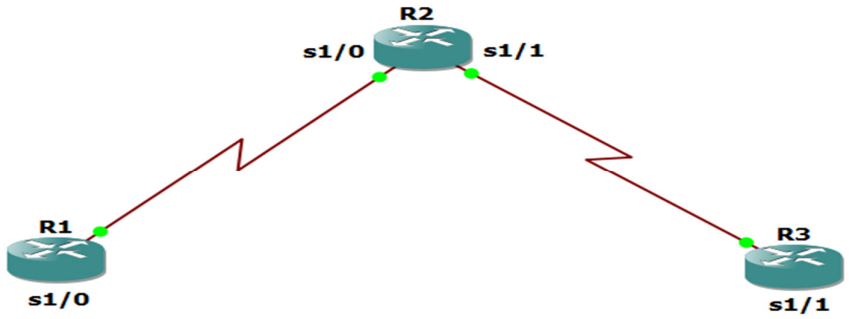
Objective:

- Secure management access.
- Configure enhanced username password security.
- Enable AAA RADIUS authentication.
- Enable secure remote management.

Topology:



Step 1: Configure loopbacks and assign addresses.

Cable the network as shown in the topology diagram. Erase the startup configuration and reload each router to clear previous configurations. Using the addressing scheme in the diagram, apply the IP addresses to the interfaces on the R1, R2, and R3 routers.

R1:

```
*Apr  1 00:31:06.103: %LINK-5-CHANGED: Interface Serial3/0, changed state to administratively down
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface Loopback 0
R1(config-if)#
*Apr  1 00:34:06.911: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface Serial 1/0
R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
R1(config-if)#exit
*Apr  1 00:36:08.003: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
R1(config-if)#exit
R1(config)#
*Apr  1 00:36:09.011: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R1(config)#exit
```

R2:

```
*Apr  1 00:31:06.151: %LINK-5-CHANGED: Interface Serial3/0, changed state to administratively down
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface Serial 1/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
*Apr  1 00:37:46.151: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
*Apr  1 00:37:47.151: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R2(config)#exit
R2#
*Apr  1 00:37:54.995: %SYS-5-CONFIG_I: Configured from console by console
R2#
```

R3:

```
inistratively down
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface loopback 0
R3(config-if)#
*Apr  1 00:40:31.279: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#exit
R3(config)#interface serial 1/1
R3(config-if)#ip address 10.2.2.2 255.255.255.252
R3(config-if)#non shutdown
             ^
% Invalid input detected at '^' marker.

R3(config-if)#no shutdown
R3(config-if)#er
*Apr  1 00:42:51.931: %LINK-3-UPDOWN: Interface Serial1/1, changed state to up
R3(config-if)#exi
*Apr  1 00:42:52.939: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/1, changed state to up
R3(config-if)#exit
R3(config)#end
R3#
```

Step 2: Configure static routes.

A. On R1, configure a default static route to ISP.

R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2
R1(config)#exit
R1#
```

B. On R3, configure a default static route to ISP.

R3(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.1

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip route 0.0.0.0 0.0.0.0 10.2.2.1
R3(config)#exit
R3#
```

C. On R2, configure two static routes.

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

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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
R2(config)#exit
R2#
*Apr  1 00:46:29.227: %SYS-5-CONFIG_I: Configured from console by console
R2#
```

D. From the R1 router, run the following Tcl script to verify connectivity.

foreach address {

192.168.1.1

10.1.1.1

10.1.1.2

10.2.2.1

10.2.2.2

192.168.3.1

} { ping $address }

```
R1#tclsh
R1(tcl)#foreach address {
+>(tcl)#192.168.1.1
+>(tcl)#10.1.1.1
+>(tcl)#10.1.1.2
+>(tcl)#10.2.2.1
+>(tcl)#10.2.2.2
+>(tcl)#192.168.3.1
+>(tcl)#} { ping $address }
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 = 1/5/8 ms
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 = 52/59/64 ms
Type escape sequence to abort.
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/59/64 ms
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 = 20/29/40 ms
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 = 16/25/36 ms
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 = 36/54/68 ms
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 = 56/58/64 ms
R1(tcl)#exit
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

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#security passwords min-length 10
R1(config)#enable secret class12345
R1(config)#exit
R1#
*Apr  1 00:51:43.879: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

Note: Passwords in this task are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

C. Configure a console password and enable login for routers. For additional security, the exec-timeout command causes the line to log out after 5 minutes of inactivity. The logging synchronous command prevents console messages from interrupting command entry.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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
R1(config)#
```

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

```
R1(config)#
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
R1(config)#
```

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)#
R1(config)#line aux 0
R1(config-line)#no exec
R1(config-line)#end
R1#
*Apr  1 00:56:46.307: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

F. Enter privileged EXEC mode and issue the show run command. Can you read the enable secret password? Why or why not?

```
R1#show run
Building configuration...

Current configuration : 2817 bytes
```

```
!
interface Serial3/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/1
 no ip address
 shutdown
 serial restart-delay 0
!
```

```
!
line con 0
 exec-timeout 5 0
 privilege level 15
 password 7 05080F1C22434D061715160118
 logging synchronous
 login
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 no exec
 stopbits 1
line vty 0 4
 exec-timeout 5 0
 password 7 05080F1C2243581D0015160118
 login
!
!
end
```

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

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#service password-encryption
R1(config)#exit
R1#
```

H. Issue the show run command. Can you read the console, aux, and vty passwords? Why or why not?

```
R1#show run
Building configuration...

Current configuration : 2817 bytes
```

```
!
interface Serial3/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/1
 no ip address
 shutdown
 serial restart-delay 0
!
```

```
!
line con 0
 exec-timeout 5 0
 privilege level 15
 password 7 05080F1C22434D061715160118
 logging synchronous
 login
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 no exec
 stopbits 1
line vty 0 4
 exec-timeout 5 0
 password 7 05080F1C2243581D0015160118
 login
!
!
end
```

I. 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#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#banner motd $Unauthorized access strictly prohibited!$
R1(config)#banner mord $Unauthorized access strictly prohibited!$
Enter TEXT message.  End with the character 'm'.
```

Router R3:

A. On R3, use the security passwords command to set a minimum password length of 10 characters.

B. Configure the enable secret encrypted password on both route.

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#security passwords min-length 10
R3(config)#enable secret class12345
R3(config)#exit
R3#
```

C. Configure a console password and enable login for routers. For additional security, the exec-timeout command causes the line to log out after 5 minutes of inactivity. The logging synchronous command prevents console messages from interrupting command entry.

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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)#
```

D. Configure the password on the vty lines for router R3.

```
R3(config)#
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)#
```

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.

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

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

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#service password-encryption
R3(config)#exit
R3#
*Apr  1 01:11:22.583: %SYS-5-CONFIG_I: Configured from console by console
R3#shown run
      ^
% Invalid input detected at '^' marker.

R3#show run
Building configuration...

Current configuration : 2800 bytes
!
! Last configuration change at 01:11:22 UTC Sat Apr 1 2023
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 10
enable secret 5 $1$27Hl$yzftj3QjIhJmQekvq899./
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
!
!
no ip domain lookup
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
```

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.

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#banner motd $Unauthorized access strictly prohibited!$
R3(config)#exit
R3#
```

Step 4: Configure enhanced username password security.

Router R1:

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
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#username JR-ADMIN secret class12345
R1(config)#username ADMIN secret class54321
R1(config)#
```

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

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

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

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

Router R3:

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:

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#username JR-ADMIN secret class12345
R3(config)#username ADMIN secret class54321
R3(config)#exit
R3#
```

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

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#line console 0
R3(config-line)#login local
R3(config-line)#exit
R3(config)#
```

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

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

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

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

User Access Verification

Username: ADMIN
Password:
% Login invalid

Username:
Username: ADMIN
Password:
% Login invalid

Username: ADMIN
Password:
R3>
R3>
R3>exit
```

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

Router R1:

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#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#aaa new-model
```

B. Configure the specifics for the first RADIUS server located at 192.168.1.101. Use **RADIUS-1-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
R1(config)#
```

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)#
R1(config)#radius server RADIUS-2
R1(config-radius-server)#radius server RADIUS-2
Warning: Address not yet configured.
R1(config-radius-server)#address ipv4 192.168.1.102
R1(config-radius-server)#key RADIUS-2-pa55w0rd
R1(config-radius-server)#exit
R1(config)#
```

D. Assign both RADIUS servers to a server group.

```
R1(config)#
R1(config)#aaa group server radius RADIUS-GROUP
R1(config-sg-radius)#
R1(config-sg-radius)#server name RADIUS-1
R1(config-sg-radius)#server name RADIUS-2
R1(config-sg-radius)#exit
R1(config)#
R1(config)#
```

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.

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)#
R1(config)#$ication login TELNET-LOGIN group RADIUS-GROUP local-case
R1(config)#
R1(config)#
```

G. Alter the VTY lines to use the TELNET-LOGIN AAA authentication method.

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

Router R3:

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.

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#aaa new-model
R3(config)#
```

B. Configure the specifics for the first RADIUS server located at 192.168.1.101. Use **RADIUS-1-pa55w0rd** as the server password.

```
R3(config)#
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)#
```

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

```
R3(config)#
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)#
```

D. Assign both RADIUS servers to a server group.

```
R3(config)#
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)#
```

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.

```
R3(config)#
R3(config)#aaa authentication login default group RADIUS-GROUP local
R3(config)#
```

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.

```
R3(config)#
R3(config)#$ication login TELNET-LOGIN group RADIUS-GROUP local-case
R3(config)#
```

G. Alter the VTY lines to use the TELNET-LOGIN AAA authentication method.

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#line vty 0 4
R3(config-line)#login authentication TELNET-LOGIN
R3(config-line)#exit
R3(config)#
```

Router R1:

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

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

Username: ADMIN
Password:

R3>
R3>exit
```

Step 6: Enabling secure remote management using SSH.

Router R1:

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
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip domain-name ccnasecurity.com
R1(config)#
```

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
```

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  1 01:43:38.991: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

D. Cisco routers support two versions of SSH:

1. SSH version 1 (SSHv1): Original version but has known vulnerabilities.

2. SSH version 2 (SSHv2): Provides better security using the Diffie-Hellman key exchange and the strong integrity-checking message authentication code (MAC).

3. Configure SSH version 2 on R1.

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

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

```
R1(config)#
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#show 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 AAAAB3NzaC1yc2EAAAADAQABAAAAgQCJWZT0SbqvpkNH+xtVLx/BpX7v0G6Rfj2Pq1pG+JFA
6mDK3EXgov/i+c691YeTQnaLx17kcNn5LaftrkWahlQkPacKL1qKSwbW0zADDzlvWfgnLHyV4wVk+ZAS
ECb8iTszv6kWD2Rv1M5enC96msp5HKRhbsP5QJynbBJfKV4dHQ==
```

Router R3:

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.

```
R3(config)#
R3(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.

```
R3(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.

```
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 2 seconds)

R3(config)#
*Apr  1 01:46:53.855: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

D. Cisco routers support two versions of SSH:

1. **SSH version 1 (SSHv1)**: Original version but has known vulnerabilities.

2. **SSH version 2 (SSHv2)**: Provides better security using the Diffie-Hellman key exchange and the strong integrity-checking message authentication code (MAC).

3. Configure SSH version 2 on R1.

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

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

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

F. Verify the SSH configuration using the show ip ssh command.

```
R3#show 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 AAAAB3NzaC1yc2EAAAADAQABAAAAgQC80QIbpsWGUxhKivUmbFxTjxpYGFCbv21W87OepDuM
RA/yMqgUVFluCXUNSRCuu4Qvu0ClcTevCgcYIKUzKpLwIwPuVclN8rJ5Vwh8+Hk7YUtyfTNS5GC6vlSM
wvmB5q3mjsVak5qoCgmoqU6aR3yYJZoTuG7yXSX47Lr6qDCCKQ==
R3#
```

Router R1:

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

```
R1#ssh -l ADMIN 10.2.2.2
Password:
% Password:  timeout expired!
[Connection to 10.2.2.2 aborted: error status 0]
R1#ssh -l ADMIN 10.2.2.2
Password:
Unauthorized access strictly prohibited!R3>
R3>en
Password:
% Access denied

R3>
[Connection to 10.2.2.2 closed by foreign host]
R1#
```

**********END**********