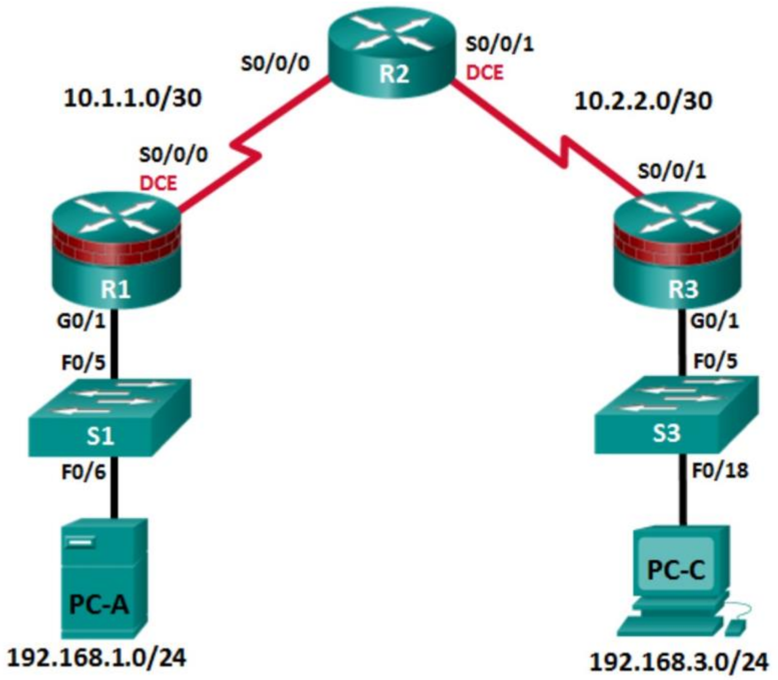
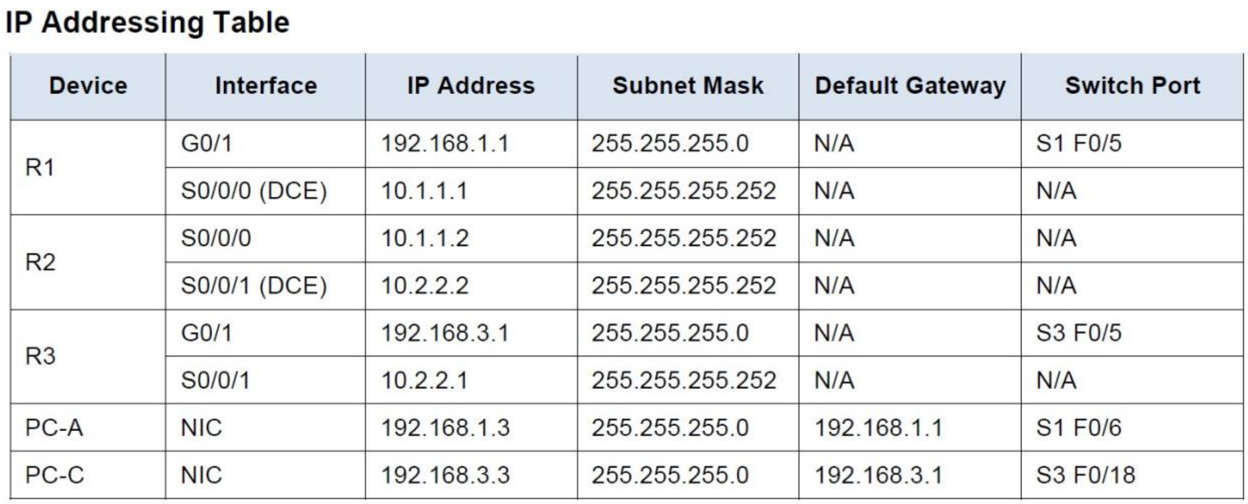
ITNE 2005
Develop Security Infrastructure

Lab Tutorial – 2 of Lesson - 2

Securing Router

Objective: Securing the Router for Administrative Access





IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

In this lab, you will perform the following tasks:

Part 1: Configure Basic Device Settings

- Cable the network as shown in the topology.
- Configure basic IP addressing for routers and PCs.
- Configure OSPF routing.
- Configure PC hosts.
- Verify connectivity betweenhosts and routers.

Part 2: Control Administrative Access for Routers

- Configure and encrypt all passwords.
- Configure a login-warning banner.
- Configure enhanced username password security.
- Configure an SSH server on a router.
- Configure an SSH client and verify connectivity.
- Configure an SCP server on a router.

Part 3: Configure Administrative Roles

- Create multiple role views and grant varying privileges.
- Verify and contrast views.

Part 4: Configure Cisco IOS Resilience and Management Reporting

- Secure the Cisco IOS image and configuration files.
- Configure SNMPv3 Security using an ACL.
- Configure a router as a synchronized time source for other devices using NTP.
- Configure Syslog support on a router.
- Install a Syslog server on a PC and enable it.
- Make changes to the router and monitor syslog results on the PC.

Part 5: Secure the Control Plane

- Configure OSPF Authentication using SHA256.
- Verify OSPF Authentication.

Part 6: Configure Automated Security Features

- Lock down a router using AutoSecure and verify the configuration.
- Contrast using AutoSecure with manually securing a router using the command line.

BACKGROUND

The router is a critical component in any network. It controls the movement of data into and out of the network and between the devices within the network. It is particularly important to protect network routers because the failure of a routing device could make sections of the network, or the entire network, inaccessible. Controlling access to routers and enabling reporting on routers is critical to network security and should be part of a comprehensive security policy.

In this lab, you will build a multi-router network and configure the routers and hosts. Use various CLI tools to secure local and remote access to the routers, analyze potential vulnerabilities, and take steps to mitigate them. Enable management reporting to monitor router configuration changes.

Note: Before beginning, ensure that the routers and switches have been erased and have no startup configurations.

Task 1: Configure Basic Device Settings

The desktop system assigned to you serves as an end-user terminal. You access and manage the lab environment from the student desktop system using GNS3 Software.

Students should perform the steps in this task individually.

In Part 1, set up the network topology and configure basic settings, such as interface IP addresses.

Step 1: Deploy router in GNS3 network.

Attach the devices, as shown in the topology diagram, and connection as necessary.

Step 2: Configure basic settings for each router.

a. Configure host names as shown in the topology plus your student ID.
b. Configure interface IP addresses as shown in the IP Addressing Table.

```
R1 Config
R1-S0000#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1-S0000(config)#interface f0/1
R1-S0000(config-if)#ip address 192.168.1.1 255.255.255.0
R1-S0000(config-if)#no shutdown
R1-S0000(config-if)#exit
R1-S0000(config)#interface s0/0
R1-S0000(config-if)#ip address 10.1.1.1 255.255.255.252
```

```
R1-S0000(config-if)#no shutdown
R1-S0000(config-if)#exit
R1-S0000(config)#exit
R1-S0000#copy running-config startup-
config Destination filename[startup-
config]? R3 Config

R3-S0000#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3-S0000(config)#interface f0/1
R3-S0000(config-if)#ip address 192.168.3.1 255.255.255.0
R3-S0000(config-if)#no shutdown
R3-S0000(config-if)#exit
R3-S0000(config)#interface s0/1
R3-S0000(config-if)#ip address 10.2.2.1 255.255.255.252
R3-S0000(config-if)#no shutdown
R3-S0000(config-if)#exit
R3-S0000(config)#exit
R3-S0000#copy running-config startup-config
    Destination filename[startup-config]?
R2 Config
R2-S0000#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2-S0000(config)#interface s0/0
R2-S0000(config-if)#ip address 10.1.1.2 255.255.255.252
R2-S0000(config-if)#no shutdown
R2-S0000(config-if)#exit
R2-S0000(config)#interface s0/1
R2-S0000(config-if)#ip address 10.2.2.2 255.255.255.252
R2-S0000(config-if)#no shutdown
R2-S0000(config-if)#exit
R2-S0000(config)#exit
R2-S0000#copy running-config startup-config
    Destination filename[startup-config]?
```

c. Configure a clock rate for routers with a DCE serial cable attached to their serial interface. R1-STUDENTID is shown here as an example.

```
R1-S0000# Conf t

R1-S0000(config)# interface S0/0

R1-S0000(config-if)# clock rate 64000

R1-S0000(config-if)# Exit

R1-S0000(config)# Exit
```

```
R3:

R3-S000        #          Conf     t

R3-S0000(config)#         interface          S0/1

R3-S0000(config-if)#      clock     rate     64000

R3-S0000(config-if)#      Exit

R3-S0000(config)#         Exit

R2:

R2-S000        #          Conf     t

R2-S0000(config)#         interface          S0/0

R2-S0000(config-if)#      clock     rate     64000

R2-S0000(config-if)#      exit

R2-S0000(config)#         interface          S0/1

R2-S0000(config-if)#      clock     rate     64000

R2-S0000(config-if)#      Exit

R2-S0000(config)#         Exit
```

d. To prevent the router from attempting to translate incorrectly entered commands as though they were host names, disable DNS lookup. R1-STUDENTID is shown here as an example.

```
R1-S000        #          Conf     t

R1-S0000(config)#         no       ip       domain-lookup

R1-S0000(config-if)#      Exit

R1-S0000(config)#         Exit

R2:

R2-S000        #          Conf     t

R2-S0000(config)#         no       ip       domain-lookup

R2-S0000(config-if)#      Exit

R2-S0000(config)#         Exit
```

R3:

```
R3-S000 # Conf t

R3-S0000(config)# no ip domain-lookup

R3-S0000(config-if)# Exit

R3-S0000(config)# Exit
```

Step 3: Configure OSPF routing on the routers.

a. Usethe router ospf command in global configuration mode to enable OSPF on R1-STUDENTID.

```
R1-S0000(config)# Conf t

R1-S0000(config)# router ospf 1
```

b. Configure the network statements for the networks on R1-STUDENTID. Use an area ID of 0.

```
R1-S0000(config-router)# network 192.168.1.0 0.0.0.255 area 0

R1-S0000(config-router)# network 10.1.1.0 0.0.0.3 area 0

R1-S0000(config-if)# Exit

R1-S0000(config)# Exit
```

c. Configure OSPF on R2-STUDENTID and R3-STUDENTID.

R3:

```
R3-S0000# Conf t
R3-S0000(config)# router ospf 1
R3-S0000(config-router)# network 192.168.3.0 0.0.0.255 area 0
R3-S0000(config-router)# network 10.2.2.0 0.0.0.3 area 0

R3-S0000(config-if)# Exit

R3-S0000(config)# Exit
```

R2:

```
R2-S0000# Conf t
R2-S0000(config)# router ospf 1
R2-S0000(config-router)# network 10.1.1.0 0.0.0.3 area 0
R2-S0000(config-router)# network 10.2.2.0 0.0.0.3 area 0

R2-S0000(config-if)# Exit

R2-S0000(config)# Exit
```

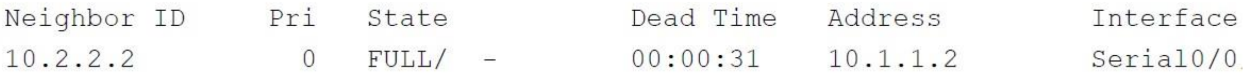
d. Issue the passive-interface command to change the f0/1 interface on R1-STUDENTID and R3-STUDENTID to passive.

```
R1-S0000# Conf t

R1-S0000(config)# router ospf 1

R1-S0000(config-router)# passive-interface f0/1

R1-S0000(config-if)# Exit

R1-S0000(config)# Exit

R3:

R3-S0000# Conf t

R3-S0000(config)# router ospf 1

R3-S0000(config-router)# passive-interface f0/1

R3-S0000(config-if)# Exit

R3-S0000(config)# Exit
```

Step 4: Verify OSPF neighbors and routing information.

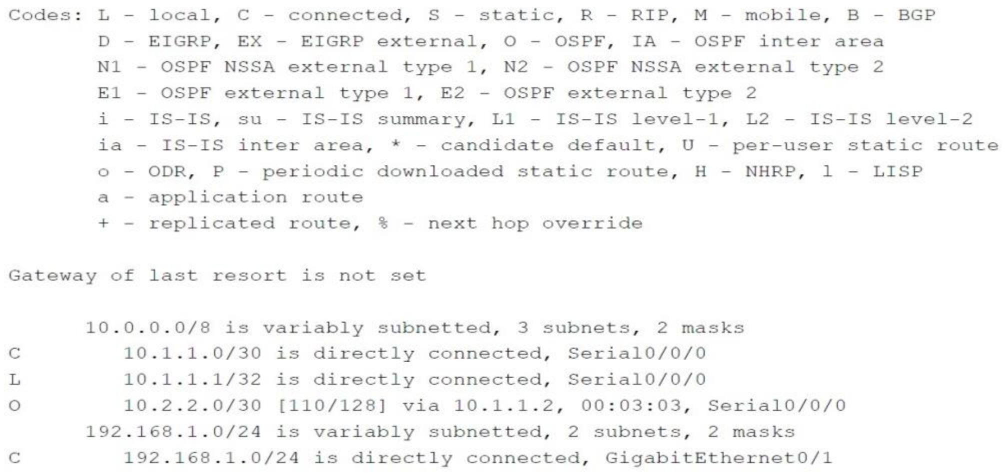
a. Issue the show ip ospf neighbor command to verify that each router lists the other routers in the network as neighbors.

```
R1-S0000 # show ip ospf neighbor
```



```
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.2.2.2          0   FULL/  -        00:00:31    10.1.1.2        Serial0/0
```

b. Issue the show ip route command to verify that all networks display in the routing table on all routers. R1-S0000 # show ip route

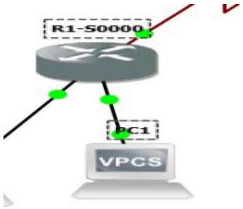


```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
O        10.2.2.0/30 [110/128] via 10.1.1.2, 00:03:03, Serial0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/1
```

Step 5: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-C as shown in the IP Addressing Table.

Deploy VPCS A: Connect to port R1 f0/1



PCA> ip 192.168.1.2/24 192.168.1.1

PCA> Save

Deploy VPCS C: Connect to R3 f0/1

PCA> ip 192.168.3.2/24 192.168.3.1

PCA> Save

Step 6: Verify connectivity between PC-A and PC-C.

a. Ping from R1-STUDENTID to R3-STUDENTID.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A, on the R1-STUDENTID-STUDENTID LAN, to PC-C, on the R3-STUDENTID LAN.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-A to PC-C you have demonstrated that OSPF routing is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the show run, show ip ospf neighbor, and show ip route commands to help identify routing protocol-related problems.

Step 7: Save the basic runningconfiguration for each router.

Save the basic running configuration for the routers as text files on your PC. These text files can be used to restore configurations later in the lab.

Task2: Control Administrative Access for Routers

- Configure and encrypt passwords.
- Configure a login-warning banner.
- Configure enhanced username password security.
- Configure enhanced virtual login security.
- Configure an SSH server on R1-STUDENTID-STUDENTID.
- Research terminal emulation client softwareand configure the SSH client.
- Configure an SCP server on R1-STUDENTID-STUDENTID.

Note: Perform all tasks on both R1-STUDENTID-STUDENTID and R3-STUDENTID. The procedures and output for R1STUDENTID are shown here.

Task 1: Configure and Encrypt Passwords on RoutersR1-STUDENTID and R3-STUDENTID.

Step 1: Configure a minimum password length for all router passwords.

Use the security passwords command to set a minimum password length of 10 characters.

```
R1-S0000# conf t

R1-S0000(config)# security passwords min-length 10



R2-S0000# conf t
```

```
R2-S0000(config)# security passwords min-length 10
```

```
R1-S0000# conf t
```

```
R3-S0000(config)# security passwords min-length 10
```

Step 2: Configure the enable secret password.

Configure the enable secret encrypted password on both routers. Use the type 9 (SCRYPT) hashing algorithm.

```
R1-S0000(config)# enable secret cisco12345
```

How does configuring an enable secret password help protect a router from being compromised by an attack?

Step 3: Configure basic console, auxiliary port, and virtual access lines.

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.

a. 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 preventsconsole messages from interrupting command entry.

Note: To avoid repetitive logins during this lab, the exec-timeout command can be set to 0 0, which preventsit from expiring. However, this is not considered a good security practice.

```
R1-S0000#                    conf          t
R1-S0000(config)#            line          console 0
R1-S0000(config-line)#       password      ciscocon
R1-S0000(config-line)#       exec-timeout  5       0
R1-S0000(config-line)#       login
R1-S0000(config-line)#       logging       synchronous
```

When you configured the password for the console line, what message was displayed?

____

____

b. Configure a new password of ciscoconpass for the console.

c. Configure a password for the AUX port for router R1-STUDENTID.

```
R1-S0000(config)#            line          aux     0
R1-S0000(config-line)#       password      ciscoauxpass
R1-S0000(config-line)#       exec-timeout  5       0
R1-S0000(config-line)#       login
```

d. Telnetfrom R2-STUDENTID to R1-STUDENTID.

```
R2-S0000>     telnet   10.1.1.1
```

Were you able to login? Explain.

____

____

What messages were displayed?

____

____

Configure the password on the vty lines for router R1-STUDENTID.

```
R1-S0000(config)#            line          vty     0       4
```

```
R1-S0000(config-line)# password ciscovtypass
R1-S0000(config-line)# exec-timeout 5 0
R1-S0000(config-line)# transport input telnet
R1-S0000(config-line)# login
```

Note: The default for vty lines is now transport input none.

Telnet from R2-STUDENTID to R1-STUDENTID again. Were you able to login this time?

____

____

Enter privileged EXEC mode and issue the show run command. Can you read the enable secret password? Explain.

____

____

Can you read the console, aux, and vty passwords? Explain.

____

____

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

Step 4: Encrypt clear text passwords.

a. Use the service password-encryption command to encrypt the console, aux, and vty passwords.

```
R1-S0000(config)# service password-encryption
```

b. Issue the show run command. Can you read the console, aux, and vty passwords? Explain.

____

____

At what level (number) is the default enable secret password encrypted? _______________

At what level (number) are the other passwords encrypted?

____

Which level of encryption is harder to crack and why?

____

____

Task 2: Configure a Login Warning Banner on Routers R1-STUDENTID and R3-STUDENTID.

Step 1: Configure a warning message to display prior to login.

a. 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-S0000(config)#       banner  motd    $Unauthorized   access  strictly    prohibited!$

R1-S0000(config)#       exit
```

b. Issue the show run command. What does the $ convert to in the output?

____

____

c. Configure Banner on R2-STUDENTID and R3-STUDENTID?

Task 3: Configure Enhanced Username Password Securityon Routers R1-STUDENTID and R3-STUDENTID.

Step 1: Investigate the options for the username command.

In global configuration mode, enter the following command:

```
R1-S0000(config)#       username        user01?
```

What options are available?

Step 2: Create a new user account with a secret password.

a. Create a new user account with SCRYPT hashing to encrypt the password.

```
R1-S0000(config)# username user01 secret user01pass
```

b. Exit global configuration mode and save your configuration.

c. Display the running configuration. Which hashing method is used for the password?

Step 3: Test the new account by logging in to the console.

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

```
R1-S0000(config)# line console 0
R1-S0000(config-line)# login local
R1-S0000(config-line)# end
R1-S0000# exit
```

b. Exit to the initial router screen which displays: R1-STUDENTID con0 is now available, Press RETURN to get started.

c. Log in using the previously defined username user01 and the password user01pass.

What is the difference betweenlogging in at the console now and previously?

After logging in, issue the show run command. Were you able to issue the command? Explain.

Enter privileged EXEC mode using the enable command. Were you prompted for a password? Explain.

Step 4: Test the new account by logging in from a Telnet session.

a. From Router2-STUDENTID, establish a Telnet session with R1-STUDENTID. Telnet is disabled by default in Windows 7. If necessary, search online for the steps to enable Telnet in Windows 7.

```
R2-S0000#    telnet    192.168.1.1
```

Were you prompted for a user account? Explain.

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

```
R1-S0000(config)#    line    vty    0    4
R1-S0000(config-line)#    login    local
```

c. From Router2-STUDENTID, telnet to R1-STUDENTID again.

```
R2-S0000#    telnet    192.168.1.1
```

Were you prompted for a user account? Explain.

d. Log in as user01 with a password of user01pass.

e. During the Telnet session to R1-STUDENTID, access privileged EXEC mode with the enable command.

What password did you use?

____

____

f. For added security, set the AUX port to use the locally defined login accounts.

```
R1-S0000(config)# line aux 0
R1-S0000(config-line)# login local
```

g. End the Telnet session with the exit command.

Task 4: Configure the SSH Server on Router R1-STUDENTID and R3-STUDENTID.

In this task, use the CLI to configure the router to be managed securely using SSH instead of Telnet. Secure Shell (SSH) is a network protocol that establishes a secure terminal emulation connection to a router or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the remote login tool of choice for network professionals.

Note: For a router to support SSH, it must be configured with local authentication, (AAA services, or username) or password authentication. In this task, you configure an SSH username and local authentication.

Step 1: Configure a domain name.

Enter global configuration mode and set the domain name.

```
R1-S0000# conf t
R1-S0000(config)# ip domain-name ccnasecurity.com
```

Step 2: Configure a privileged user for login from the SSH client.

a. Use the username command to create the user ID with the highest possible privilege level and a secret password.

```
R1-S0000(config)# username admin privilege 15 secret cisco12345
```

Note: Usernames are not case sensitive by default. You will learn how to make usernames case sensitive.

b. Exit to the initial router login screen. Log in with the username admin and the associated password. What was the router prompt after you entered the password?

____

____

Step 3: Configure the incoming vty lines.

Specify a privilege level of 15 so that a user with the highest privilege level (15) will default to privileged EXEC mode when accessing the vty lines. Other users will default to user EXEC mode. Use the local user accounts for mandatory login and validation and accept only SSH connections.

```
R1-S0000(config)# line vty 0 4
R1-S0000(config-line)# privilege level 15
R1-S0000(config-line)# login local
R1-S0000(config-line)# transport input ssh
R1-S0000(config-line)# exit
```

Note: The login local command should have been configured in a previous step. It is included here to provide all commands, if you are doing this for the first time.

Note: If you add the keyword telnet to the transport input command, users can log in using Telnet as well as SSH, however, the router will be less secure. If only SSH is specified, the connecting host must have an SSH client installed.

Step 4: Erase existing key pairs on the router.

```
R1-S0000(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 the router.

The router uses the RSA key pair for authentication and encryption of transmitted SSH data.

a. 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-S0000(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1-STUDENTID.ccnasecurity.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1-S0000(config)#
*Dec 16 21:24:16.175: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

b. Issue the ip ssh version 2 command to force the use of SSH version 2.

```
R1-S0000(config)# ip ssh version 2
R1-S0000(config)# exit
```

Note: The details of encryption methods later.

Step 6: Verify the SSH configuration.

a. Use the show ip ssh command to see the current settings.

```
R1-S0000# show ip ssh
```

b. Fill in the following information based on the output of the show ip ssh command.

SSH version enabled:____

Authentication timeout:____

Authentication retries: ____

Step 7: Configure SSH timeouts and authentication parameters.

The default SSH timeouts and authentication parameters can be altered to be more restrictive using the following commands.

```
R1-S0000(config)# ip ssh time-out 90
R1-S0000(config)# ip ssh authentication-retries 2
```

Step 8: Save the running-config to the startup-config.

```
R1-S0000# copy running-config startup-config
```

Task 5: Research Terminal Emulation Client Software and Configure the SSH Client.

Step 1: Research terminal emulation client software.

Conduct a web search for freeware terminal emulation client software, such as TeraTerm or PuTTy. What are some capabilities of each?

____

____

____

____

____

____

____

____

Step 2: Verify SSH connectivity to R1 from R2.

a. From Router2-STUDENTID, telnet to R1-STUDENTID again.

```
R2-S0000# ssh –l admin 192.168.1.1
```

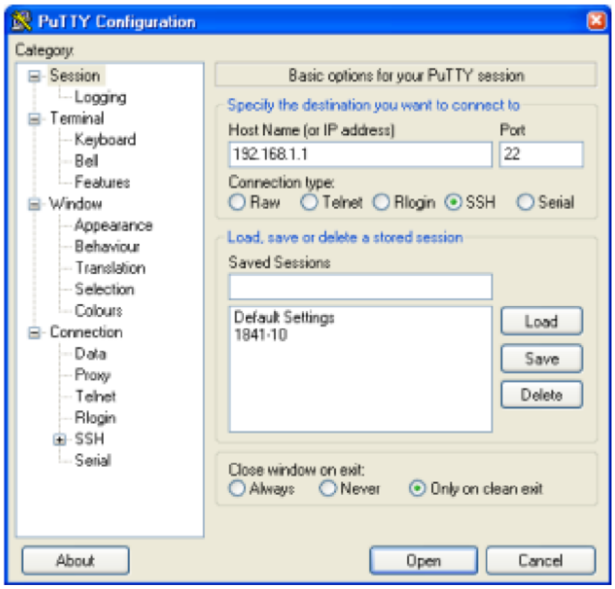
User cisco12345 as password

Or Use Host A

Launch PuTTY by double-clicking the putty.exe icon.

b. Input the R1 F0/1 IP address 192.168.1.1 in the Host Name (or IP address) field.

c. Verify that the SSH radio button is selected



Host Name (or IP address): 192.168.1.1 Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

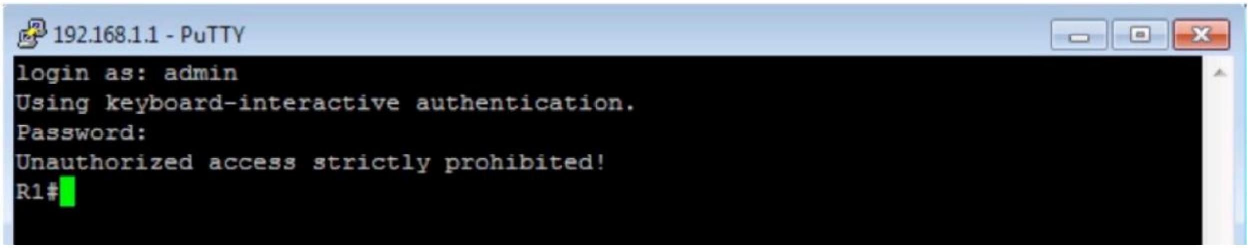
Saved Sessions: Default Settings, 1841-10

Close window on exit: ○ Always ○ Never ● Only on clean exit

d. Click Open.

e. In the PuTTY Security Alert window, click Yes.

f. Enter the admin username and password cisco12345 in the PuTTY window.



```
login as: admin
Using keyboard-interactive authentication.
Password:
Unauthorized access strictly prohibited!
R1#
```

At the R1 privileged EXEC prompt, enter the show users command.

R1-S0000# show users

What users are connected to router R1 at this time?

____

____

____

h. Close the PuTTY SSH session window or Telent from R2-StudentID.

i. Try to open a Telnet session to your router from PC-A or R2-S0000. Were you able to open the Telnet session?

Explain.

____

____

____

Open a PuTTY SSH session to the router from PC-A. Enter the user01 username and password user01pass in the PuTTY window to try connecting for a user who does not have privilege level of 15.

If you were able to login, what was the prompt?

____

____

k. Use the enable command to enter privilegeEXEC mode and enter the en