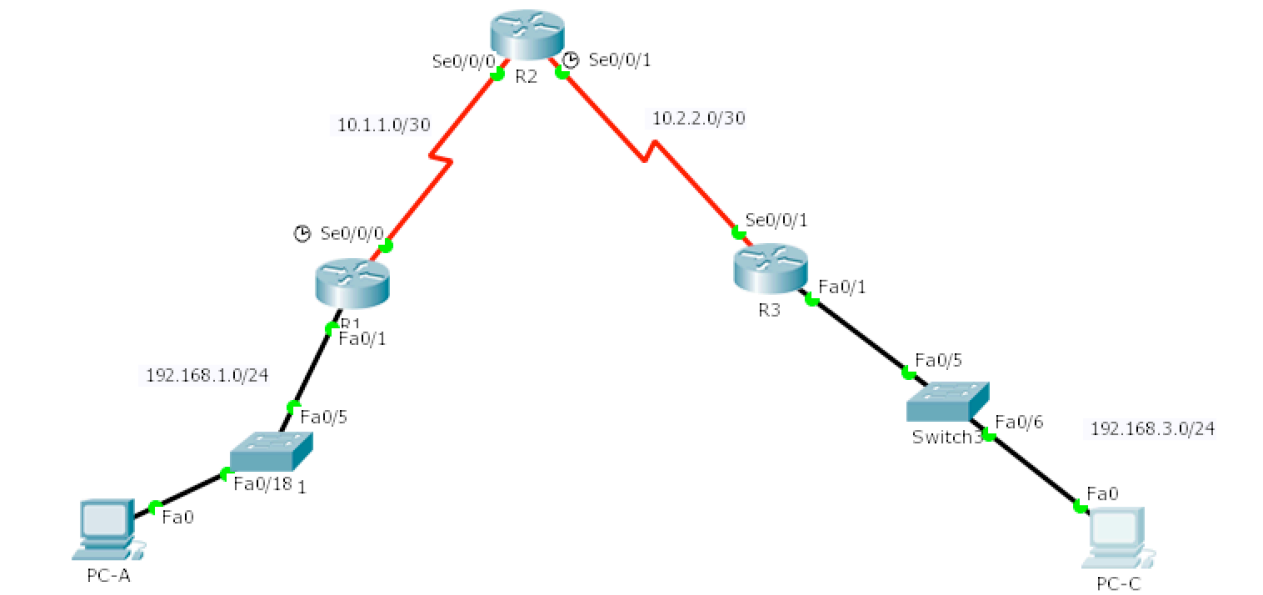


Topology



IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	FA0/1	192.168.1.1	255.255.255.0	N/A	S1 FA0/5
	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	FA0/1	192.168.3.1	255.255.255.0	N/A	S3 FA0/5
	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 FA0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 FA0/18

Control Administrative Access for Routers

In this lab, you will:

- Configure and encrypt passwords.
- Configure a login warning banner.
- Configure enhanced username password security.
- Configure enhanced virtual login security.
- Configure an SSH server on router R1 using the CLI.

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

Task 1. Configure and Encrypt Passwords on Routers R1 and R3

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

Step 2: Configure the enable secret password.

Configure the enable secret encrypted password on both routers.

```
R1(config)#enable secret cisco
```

You should receive the following message.

```
% Password too short - must be at least 10 characters.  
Password not configured.
```

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

How does configuring an enable secret password help protect a router from being compromised by an attack? Would you recommend this password in a production network? Why not? (answer on next page)

Step 3: Configure basic console 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**.
- b. 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. However, this is not considered a good security practice.

```
R1(config)#line console 0
R1(config-line)#password ciscocon
```

When you configured the password for the console line, what message was displayed? Configure a new password of **ciscoconpass** for the console.

```
R1(config-line)#exec-timeout ?
<0-35791> Timeout in minutes
```

```
R1(config-line)#exec-timeout 5 0
R1(config-line)#logging synchronous
```

- a. Telnet from R2 to R1.

```
R2>telnet 10.1.1.1
```

Were you able to login? Why or why not?

What messages were displayed?

- b. 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
```

- c. Telnet from R2 to R1 again. Were you able to login this time? (not in cleartext)
- d. Enter privileged EXEC mode and issue the show run command. Can you read the enable secret password? Why or why not?
Can you read the console and vty passwords? Why or why not? (in cleartext)
- e. Repeat the configuration portion of steps 3a through 3g on router R3.

Step 4: Encrypt clear text passwords.

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

```
R1(config)# service password-encryption
```
- Issue the **show run** command. Can you read the console, and vty passwords? Why or why not?
- At what level (number) is the enable secret password encrypted? (md5)
- At what level (number) are the other passwords encrypted? (Level 7)
- Which level of encryption is harder to crack and why?

(If that digit is a 7, the password has been encrypted using the weak algorithm. If the digit is a 5, the password has been hashed using the stronger MD5 algorithm.)

However, visit the web URL:

<http://www.ifm.net.nz/cookbooks/passwordcracker.html>

Take the type 7 password, such as the text above in red, and paste it into the box below and click "Crack Password".

Type 7 Password:	0822455D0A1606181C1B0D1739
<input type="button" value="Crack Password"/>	
Plain text:	ciscoconpass

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

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

- 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 $Unauthorized access strictly  
prohibited and prosecuted to the full extent of the law$  
R1(config)#exit
```

- Issue the **show run** command. What does the \$ convert to in the output?
- Exit privileged EXEC mode using the **disable** or **exit** command and press **Enter** to get started. Does the MOTD banner look like what you created with the **banner motd** command?

Note: If the MOTD banner is not as you wanted it, recreate it using the **banner motd** command.

Task 3. Configure Enhanced Username Password Security on Routers R1 and R3.

Step 1: Investigate the options for the username command.

In global configuration mode, enter the following command:

```
R1(config)#username user01 password ?
```

What options are available?

Step 2: Create a new user account using the username command.

- a. Create the user01 account, specifying the password with no encryption.

```
R1(config)#username user01 password 0 user01pass
```

- b. Use the **show run** command to display the running configuration and check the password that is enabled.

You still cannot read the password for the new user account. Even though unencrypted (0) was specified because the **service password-encryption** command is in effect.

Step 3: Create a new user account with a secret password.

- a. Create a new user account with MD5 hashing to encrypt the password.

```
R1(config)#username user02 secret user02pass
```

- b. Exit global configuration mode and save your configuration.
- c. Display the running configuration. Which hashing method is used for the password?

Step 4: Test the new account by logging in to the console.

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

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

- b. Exit to the initial router screen which displays: **R1 con0 is now available, Press RETURN to get started.**
- c. Log in using the user01 account and password previously defined.
What is the difference between logging in at the console now and previously?
- d. After logging in, issue the **show run** command. Were you able to issue the command? Why or why not?
- e. Enter privileged EXEC mode using the **enable** command. Were you prompted for a password? Why or why not?

Step 5: Test the new account by logging in from a Telnet session.

- a. From PC-A, establish a Telnet session with R1.

PC-A>**telnet 192.168.1.1**

Were you prompted for a user account? Why or why not?

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

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

- c. From PC-A, telnet to R1 again.

PC-A>**telnet 192.168.1.1**

Were you prompted for a user account?

Why or why not? .

- d. Log in as user01 with a password of user01pass.
e. While telnetted to R1, access privileged EXEC mode with the **enable** command.
What password did you use?
f. End the Telnet session with the **exit** command.

Task 4. Configure Enhanced Virtual Login Security on Routers R1 and R3

Step 1: Configure the router to watch for login attacks.

Use the **login block-for** command to help prevent brute-force login attempts from a virtual connection, such as Telnet, SSH, or HTTP. This can help slow down dictionary attacks and help protect the router from a possible DoS attack.

- a. From the user EXEC or privileged EXEC prompt, issue the **show login** command to see the current router login attack settings.

```
R1#show login  
No login delay has been applied.  
No Quiet-Mode access list has been configured.  
Router NOT enabled to watch for login Attacks
```

- b. Use the **login block-for** command to configure a 60 second login shutdown (quiet mode timer) if two failed login attempts are made within 30 seconds.

```
R1(config)#login block-for 60 attempts 2 within 30
```

- c. Exit global configuration mode and issue the **show login** command.

```
R1#show login
```

Is the router enabled to watch for login attacks?

What is the default login delay?

Step 2: Configure the router to log login activity.

- a. Configure the router to generate system logging messages for both successful and failed login attempts. The following commands log every successful login and log failed login attempts after every second failed login.

```
R1(config)#login on-success log  
R1(config)#login on-failure log
```

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

- b. Issue the **show login** command. What additional information is displayed?

Step 3: Test the enhanced login security login configuration.

- a. From PC-A, establish a Telnet session with R1.

```
PC-A> telnet 10.1.1.1
```

- b. Attempt to log in with the wrong user ID or password two times. What message was displayed on PC-A after the second failed attempt?

What message was displayed on the router R1 console after the second failed login attempt?

- c. From PC-A, attempt to establish another Telnet session to R1 within 60 seconds. What message was displayed on PC-A after the attempted Telnet connection?

What message was displayed on router R1 after the attempted Telnet connection?

```
% Connection refused by remote host
```

- d. Issue the **show login** command within 60 seconds. What additional information is displayed?

Using the CLI

In this task, you 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#conf t
R1 (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 (config) #username admin privilege 15 secret cisco12345
```

- b. Exit to the initial router login screen, and log in with this username. 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(config)#line vty 0 4
R1(config-line)#privilege level 15
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
```

Note: The **login local** command should already be configured in a previous step. It is included here to provide all commands if you were 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(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.

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
```

```
How many bits...: 1024
```

```
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-
exportable...[OK]
```

```
R1(config)#
```

```
*Dec 16 21:24:16.175: %SSH-5-ENABLED: SSH 1.99 has been
enabled
```

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

Step 6: Verify the SSH configuration.

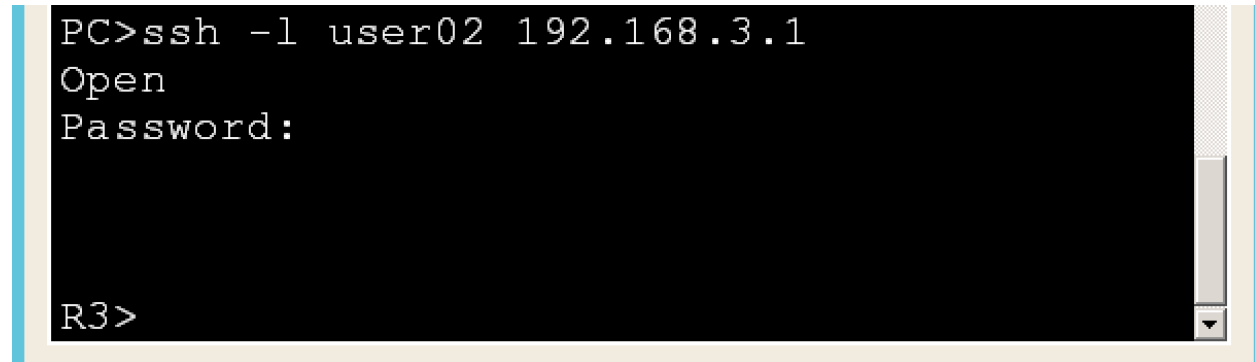
- Use the **show ip ssh** command to see the current settings.

```
R1#show ip ssh
```

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

SSH version enabled:
Authentication timeout:
Authentication retries:

Test from a PC: make sure you are using "L" in the ssh command, not the numeral 1...so to test user02 user logging in via SSH into R3 from PC1 do the following from command prompt.

A screenshot of a terminal window with a black background and white text. The text shows a command prompt for PC1 where the command 'ssh -l user02 192.168.3.1' has been entered. The output shows 'Open' and 'Password:' on separate lines. At the bottom left, the prompt 'R3>' is visible, indicating the connection was successful. A vertical scrollbar is on the right side of the terminal window.

```
PC>ssh -l user02 192.168.3.1
Open
Password:
R3>
```

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

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

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

Extended task:

Can you get PC-A to communicate (ping) with PC-C? Tip: use the OSPF routing protocol to help!