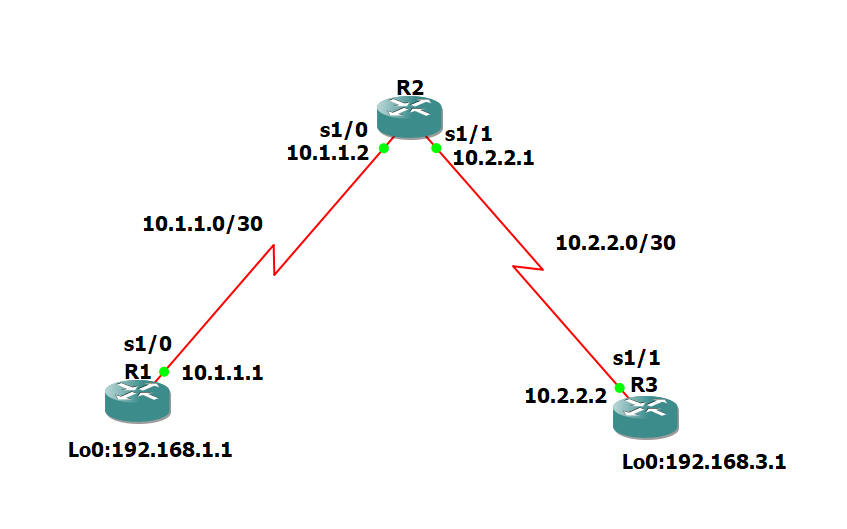
**Practical 4**

**Aim:- Secure the Management Plane**

**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.

**Router R1 Console**

conf t

hostname R1

interface Loopback 0

description R1 LAN

ip address 192.168.1.1 255.255.255.0

exit

interface Serial1/0

description R1 --> R2

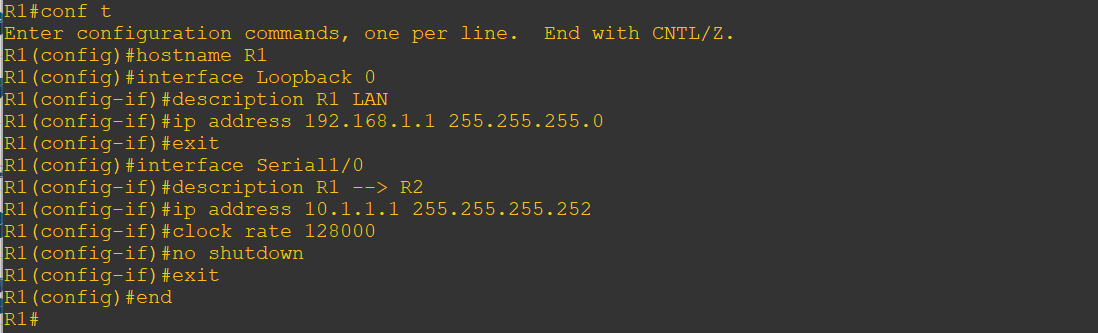
ip address 10.1.1.1 255.255.255.252

clock rate 128000

no shutdown

exit

end



**Router R2 Console**

conf t

hostname R2

interface Serial1/0

description R2 --> R1

ip address 10.1.1.2 255.255.255.252

no shutdown

exit

interface Serial1/1

description R2 --> R3

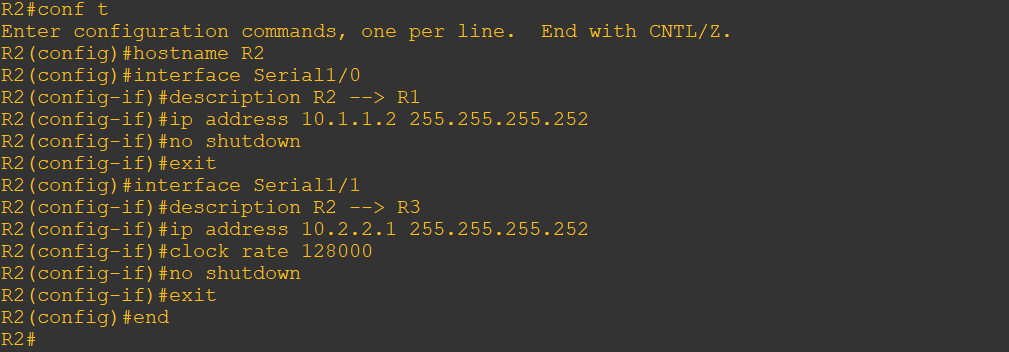
ip address 10.2.2.1 255.255.255.252

clock rate 128000

no shutdown

exit

end



**Router R3 Console**

conf t

hostname R3

interface Loopback0

description R3 LAN

ip address 192.168.3.1 255.255.255.0

exit

interface Serial1/1

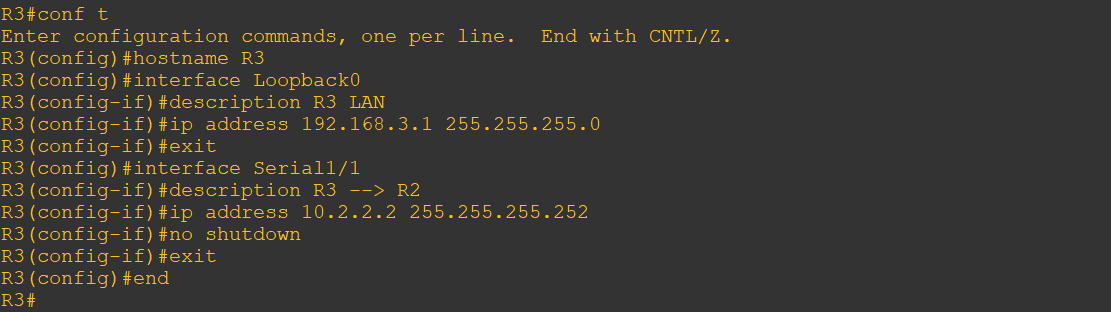
description R3 --> R2

ip address 10.2.2.2 255.255.255.252

no shutdown

exit

end



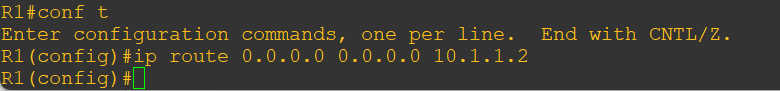
**Step 2:- Configure Static Routes.**

a) On R1, configure a default static route to R2.

**Router R1 Console**

conf t

ip route 0.0.0.0 0.0.0.0 10.1.1.2

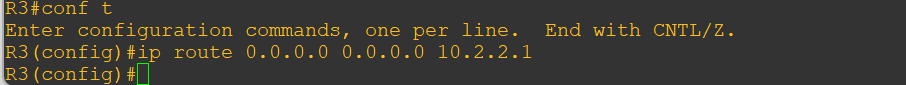


b) On R3, configure a default static route to R2.

**Router R3 Console**

conf t

ip route 0.0.0.0 0.0.0.0 10.2.2.1



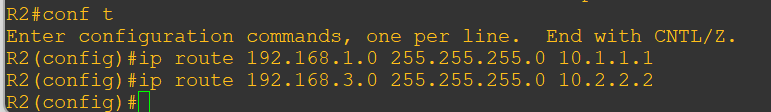
c) On R2, configure two static routes

**Router R2 Console**

conf t

ip route 192.168.1.0 255.255.255.0 10.1.1.1

ip route 192.168.3.0 255.255.255.0 10.2.2.2



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

tclsh

foreach address {

192.168.1.1

10.1.1.1

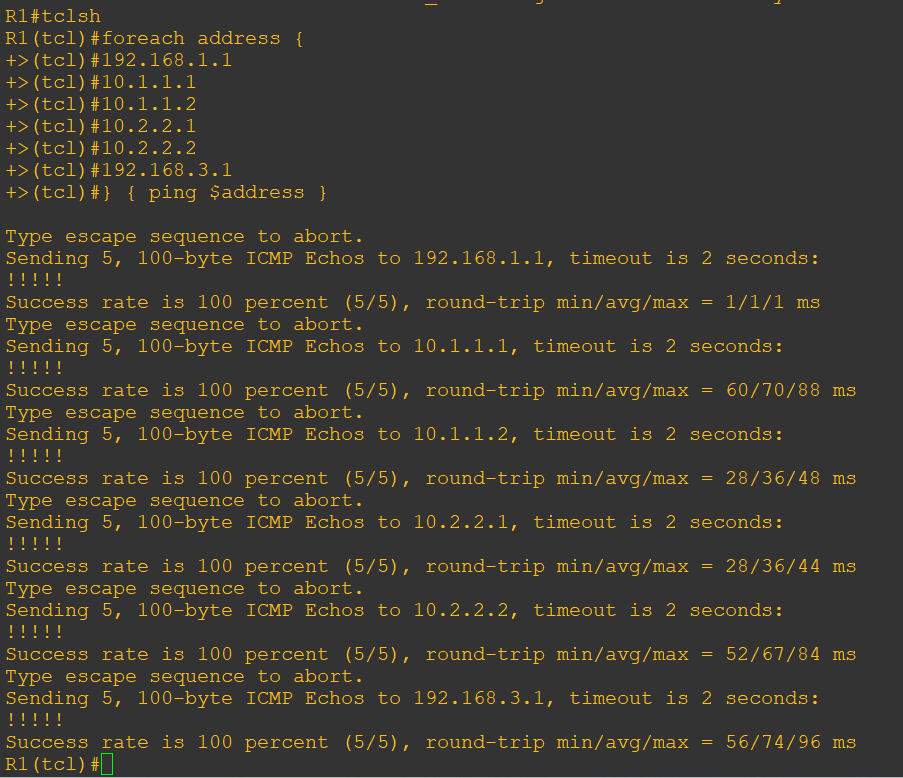
10.1.1.2

10.2.2.1

10.2.2.2

192.168.3.1

} { ping $address }



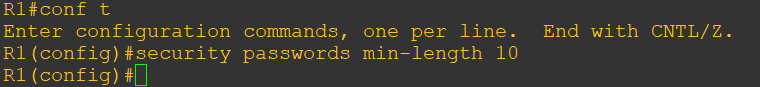
**Step 3:- Secure management access.**

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

**Router R1 Console**

conf t

security passwords min-length 10



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

**Router R1 Console**

enable secret class12345



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.

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.

**Router R1 Console**

line console 0

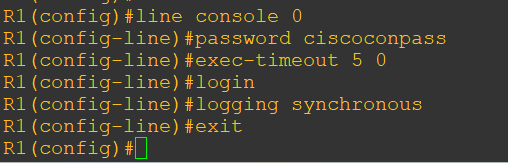
password ciscoconpass

exec-timeout 5 0

login

logging synchronous

exit



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

**Router R1 Console**

line vty 0 4

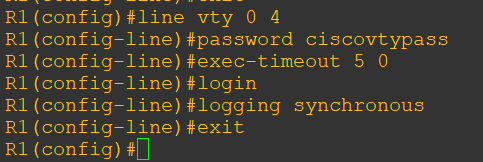
password ciscovtypass

exec-timeout 5 0

login

logging synchronous

exit



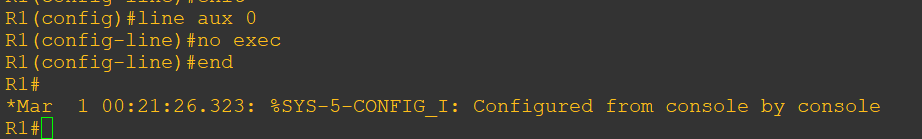
e) The aux port is a legacy port used to manage a router remotely using a modem and is hardly ever used. Therefore, disable the aux port.

**Router R1 Console**

line aux 0

no exec

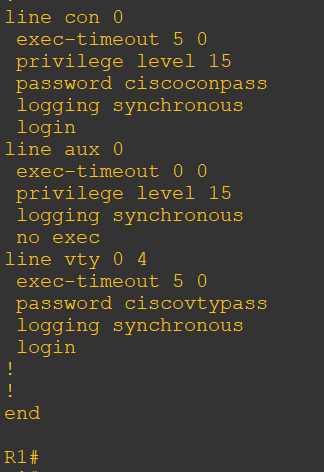
end



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

**Router R1 Console**

show run

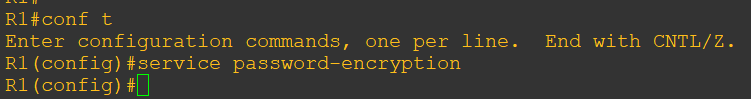


g) Use the **service password-encryption** command to encrypt the line console and vty passwords.

**Router R1 Console**

conf t

service password-encryption

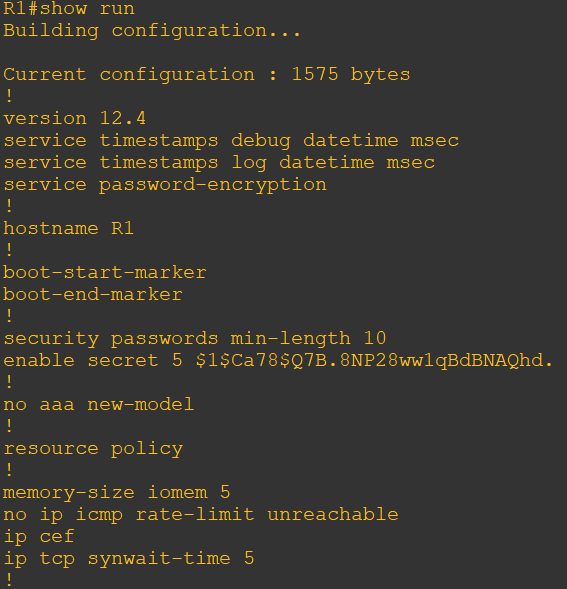


Note:- Password encryption is applied to all the passwords, including the username passwords, the authentication key passwords, the privileged command password, the console and the virtual terminal line access passwords, and the BGP neighbor passwords.

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

**Router R1 Console**

show run



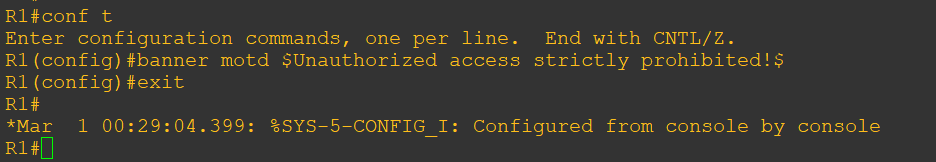
Note:- Type 7 passwords are encrypted using a Vigenère cipher which can be easily reversed. Therefore this command primarily protects from shoulder surfing attacks.

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.

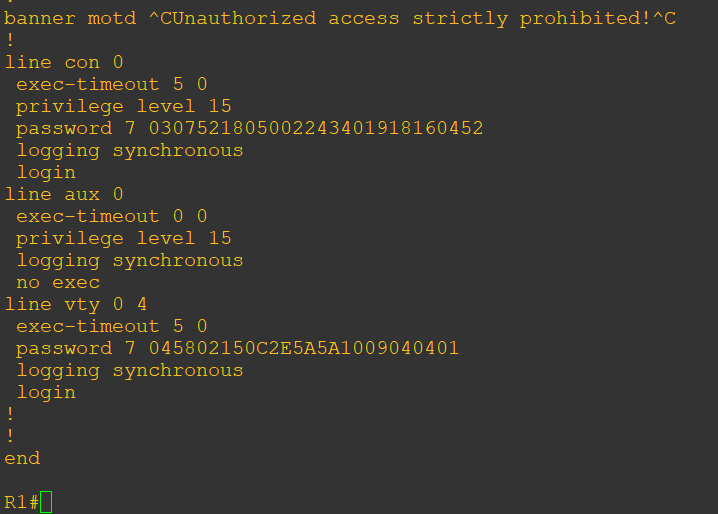
Router R1 Console

banner motd $Unauthorized access strictly prohibited!$

exit



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



k) 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? If the MOTD banner is not as you wanted it, recreate it using the banner motd command.

l) Repeat the configuration portion of steps 3a through 3k on router R3.

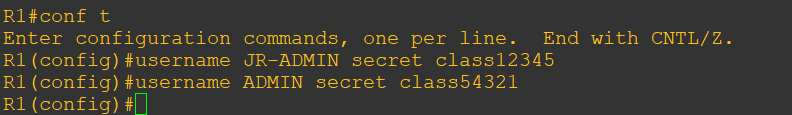
Step 4:- Configure enhanced username password security. To increase the encryption level of console and VTY lines, it is recommended to enable authentication using the local database. The local database consists of usernames and password combinations that are created locally on each device. The local and VTY lines are configured to refer to the local database when authenticating a user.

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:

Router R1 Console

username JR-ADMIN secret class12345

username ADMIN secret class54321



Note:- An older method for creating local database entries is to use the **username name password password** command.

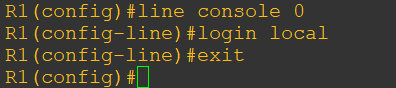
b) Set the console line to use the locally defined login accounts.

**Router R1 Console**

line console 0

login local

exit



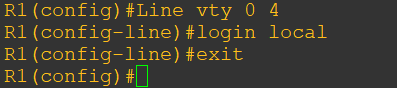
c) Set the vty lines to use the locally defined login accounts.

**Router R1 Console**

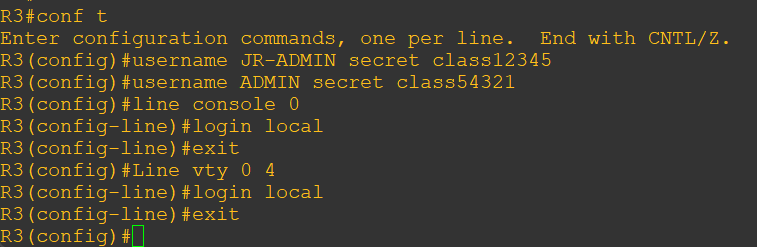
Line vty 0 4

login local

exit



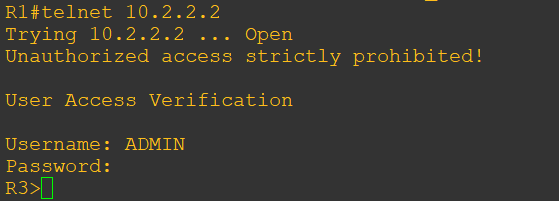
d) Repeat the steps 4a to 4c on R3.



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

**Router R1 Console**

telnet 10.2.2.2



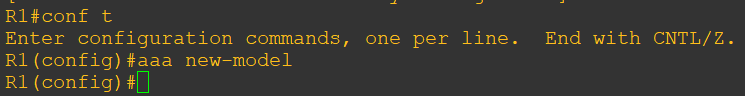
**Step 5:- Enabling AAA RADIUS Authentication with Local User for Backup.**

Authentication, authorization, and accounting (AAA) is a standards-based framework that can be implemented to control who is permitted to access a network (authenticate), what they can do on that network (authorize), and audit what they did while accessing the network (accounting).

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.

**Router R1 Console**

aaa new-model



Note:- Although the following configuration refers to two RADIUS servers, the actual RADIUS server implementation is beyond the scope. Therefore, the goal of this step is to provide an example of how to configure a router to access the servers.

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

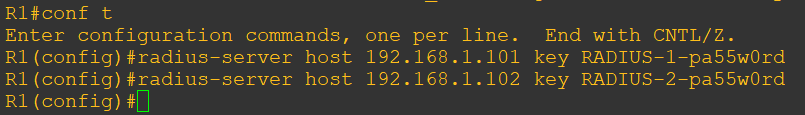
**Router R1 Console**

radius-server host 192.168.1.101 key RADIUS-1-pa55w0rd

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

**Router R1 Console**

radius-server host 192.168.1.102 key RADIUS-2-pa55w0rd



d) Assign both RADIUS servers to a server group.

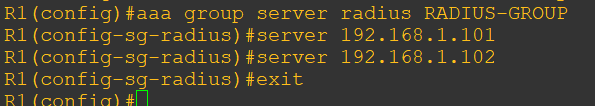
**Router R1 Console**

aaa group server radius RADIUS-GROUP

server 192.168.1.101

server 192.168.1.102

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.

**Router R1 Console**

aaa authentication login default group RADIUS-GROUP local



Note:- Once this command is configured, all line access methods default to the default authentication method. The local option enables AAA to refer to the local database. Only the password is case sensitive.

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.

**Router R1 Console**

aaa authentication login TELNET-LOGIN group RADIUS-GROUP local-case



Note:- Unlike the local option that makes the password is case sensitive, local-case makes the username and password case sensitive.

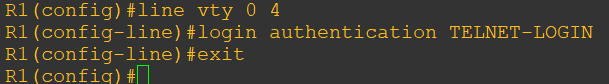
g) Alter the vty lines to use the TELNET-LOGIN AAA authentication method.

**Router R1 Console**

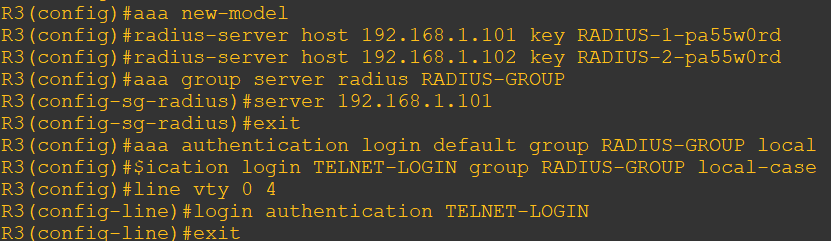
line vty 0 4

login authentication TELNET-LOGIN

exit



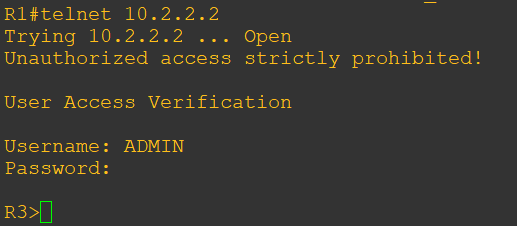
h) Repeat the steps 5a to 5g on R3.



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

**Router R1 Console**

telnet 10.2.2.2



Note:- Use password as class54321.

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

Step 6:- Enabling secure remote management using SSH Traditionally, remote access on routers was configured using Telnet on TCP port 23. However, Telnet was developed in the days when security was not an issue; therefore, all Telnet traffic is forwarded in plaintext.

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.

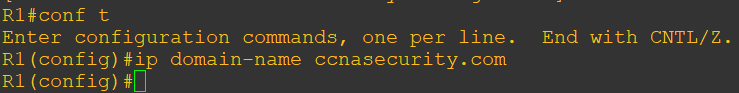
Note:- For a router to support SSH, it must be configured with local authentication, (AAA services, or username) or password authentication. In this task, you configure an SSH username and local authentication.

In this step, you will enable R1 and R3 to support SSH instead of Telnet.

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.

**Router R1 Console**

ip domain-name ccnasecurity.com

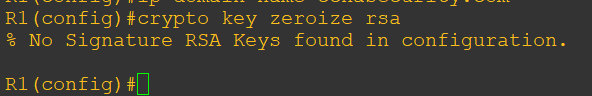


b) The router uses the RSA key pair for authentication and encryption of transmitted SSH data. Although optional it may be wise to erase any existing key pairs on the router.

**Router R1 Console**

crypto key zeroize rsa

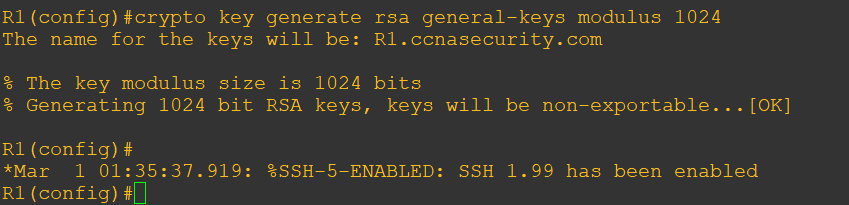
Note:- If no keys exist, you might receive this message: % No Signature RSA Keys found in configuration.



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.

Router R1 Console

crypto key generate rsa general-keys modulus 1024



d) Cisco routers support two versions of SSH:

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

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

The default setting for SSH is SSH version 1.99. This is also known as compatibility mode and is merely an indication that the server supports both SSH version 2 and SSH version 1. However, best practices are to enable version 2 only.

Configure SSH version 2 on R1.

**Router R1 Console**

ip ssh version 2



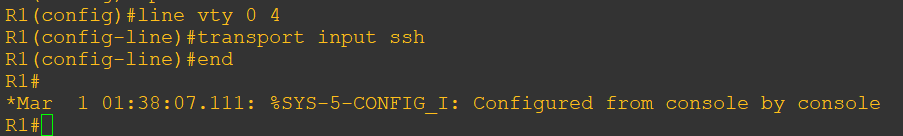
e) Configure the vty lines to use only SSH connections.

**Router R1 Console**

line vty 0 4

transport input ssh

end



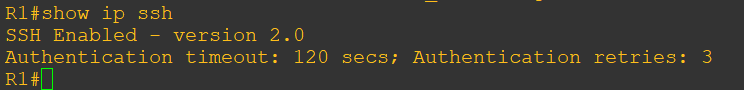
Note:- SSH requires that the **login local** command be configured. However, in the previous step we enabled AAA authentication using the TELNET-LOGIN authentication method, therefore **login local** is not necessary.

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.

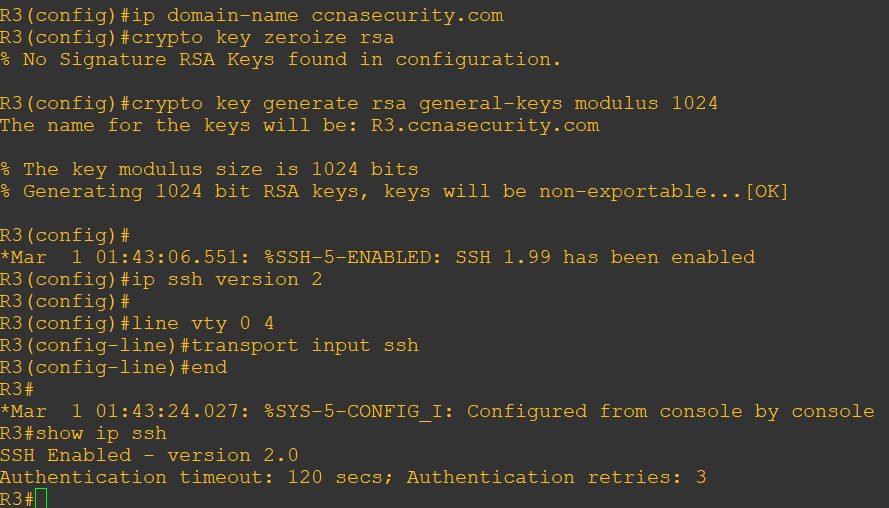
f) Verify the SSH configuration using the **show ip ssh** command.

**Router R1 Console**

show ip ssh



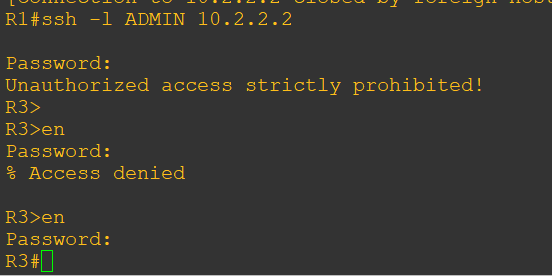
g) Repeat the steps from 6a to 6f on R3



h) 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.

**Router R1 Console**

ssh –l ADMIN 10.2.2.2



Note:- After running ssh command use password as class54321 and after entering into R3 consloe use password as class12345.