

1. Configure the device name.

2. Secure privileged EXEC mode

1000

5. Secure user EXEC mode.

```
Router(config)# line co
```

4. Secure remote Telnet / SSH access.

```
Router(config-line)# line vty 0
```

```
Router(config-line)# transport input {ssh | telnet}
```

5. Secure all passwords in the config file.

```
Router(config)# service password-encryption
```

6. Provide legal notification.

What are the learning objectives?


```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)# hostname R1
R1(config)#
```

All router access should be secured. Privileged EXEC mode provides the user with complete access to the device and its configuration. Therefore, it is the most important mode to secure.

```
R1(config)# enable secret class
R1(config)#
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1(config)#
R1(config)# service password-encryption
R1(config)#
```

```
R1(config)# banner motd #
Enter TEXT message. End with a new line and the #
*****
WARNING: Unauthorized access is prohibited!
*****
#
R1(config)#
```

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```


- Configure the device name.
- Secure the privileged EXEC mode.
- Secure and enable remote SSH and Telnet access.
- Secure all plaintext passwords.
- Provide legal notification.

 Configure Initial Router Settings

 Configure Initial Router Settings