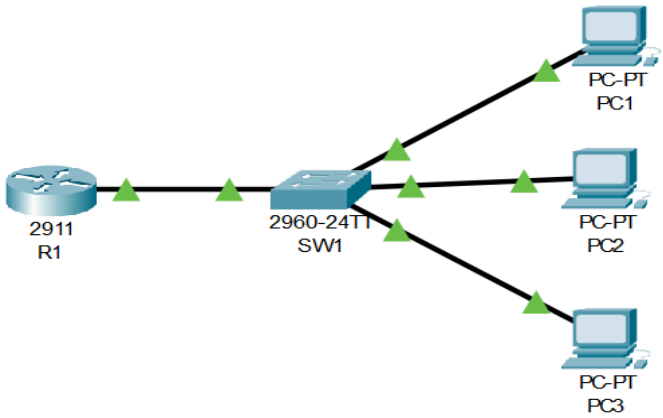

1. Lets again configure the hosts name of sw and r1 to their respective names, remember this is important for troubleshooting and device management

R1: #Hostname R1
SW1: #Hostname SW1

2. In this lab we will be setting up non-encrypted password on the router and switch

R1: #enable password “CCNA”
SW1: #enable password “CCNA”

Note that setting these passwords like this is not the best for security because you can see them in the running config: #Do sh run

```
r1(config)#do sh run
Building configuration...

Current configuration : 711 bytes
!
version 15.1
no service timestamps log datetime m
no service timestamps debug datetime
no service password-encryption
!
hostname r1
!
!
!
enable password CCNA
!
```

3. Now let's make sure all current and future passwords are encrypted

We can enter a command that will always encrypt and hash any future and current password entered into the running config we have to enter this command:

#service password-encryption

This is what the output looks on that plain text password we used earlier

```
!
enable password 7 0822455D0A16
!
```

Now when you exit and reenter the router or switch you will be prompted with a a password

4. Now let make a more secure password on the router and the switch

We can accomplish this by doing the command on both router and switch:
#Enable Secret Cisco
By doing this we can now see that the password is not stored in plaintext in the running configuration and it is more secure because it uses md5 hashing instead of encryption level 7 we can see the new output of the command in the running config

```
r1(config)#do sh running
Building configuration...

Current configuration : 758 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname r1
!
!
!
enable secret 5 $1$mERr$YlCkLMcTYWwkFlCcndtll.
enable password CCNA
```

The enable secret is more secure therefore taking priority over the enable password.