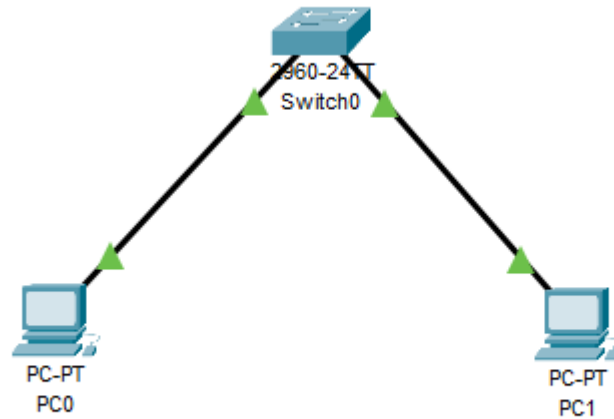


7 . Configure a management VLAN and assign an IP address for remote access. Test SSH or Telnet access to the switch.

Network topology :



Configure the Management VLAN on the Switch :

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 99
Switch(config-vlan)#name Management
Switch(config-vlan)#exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 99
Switch(config-if)#exit
Switch(config)#interface vlan 99
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#
Switch(config)#ip default-gateway 192.168.1.254
Switch(config)#exit
```

Configuring SSH on the switch :

```
Switch#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW1
SW1(config)#ip domain-name example.com
SW1(config)#crypto key generate rsa
The name for the keys will be: SW1.example.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
    a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

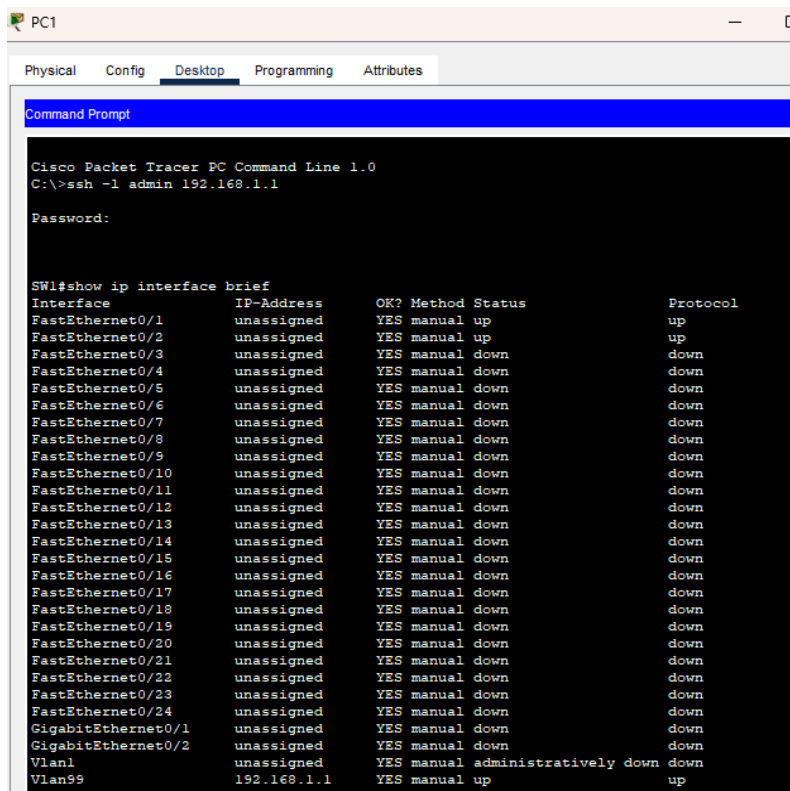
SW1(config)#ip ssh version 2
*Mar 1 0:6:31.704: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW1(config)#username admin privilege 15 secret Cisco123
SW1(config)#
SW1(config)#line vty 0 4
SW1(config-line)#transport input ssh
SW1(config-line)#login local
SW1(config-line)#exit
SW1(config)#
```

For the above configuration key size is taken as 1024

With having SSH version 2

Create a user with security key as Cisco123

TESTING SSH Command from pc1 to switch :



```

SW1#show ssh
Connection      Version Mode Encryption      Hmac      State      Username
0               1.99   IN   aes128-cbc      hmac-shal  Session Started  admin
0               1.99   OUT  aes128-cbc      hmac-shal  Session Started  admin
%No SSHv1 server connections running.
SW1#
SW1#show running-config
Building configuration...

Current configuration : 1348 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW1
!
!
!
ip ssh version 2
ip domain-name example.com
!
username admin secret 5 $1$mERr$RldxcCZsTFTETUyRaA50
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
 switchport access vlan 99
 switchport mode access
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!

```

Final learnings :

Management VLAN (VLAN 99) allows remote access to the switch.

SSH is more secure than Telnet.

Use 'show ssh' & 'show running-config' to verify settings.

Test SSH using 'ssh -l admin 192.168.1.1' from a PC.