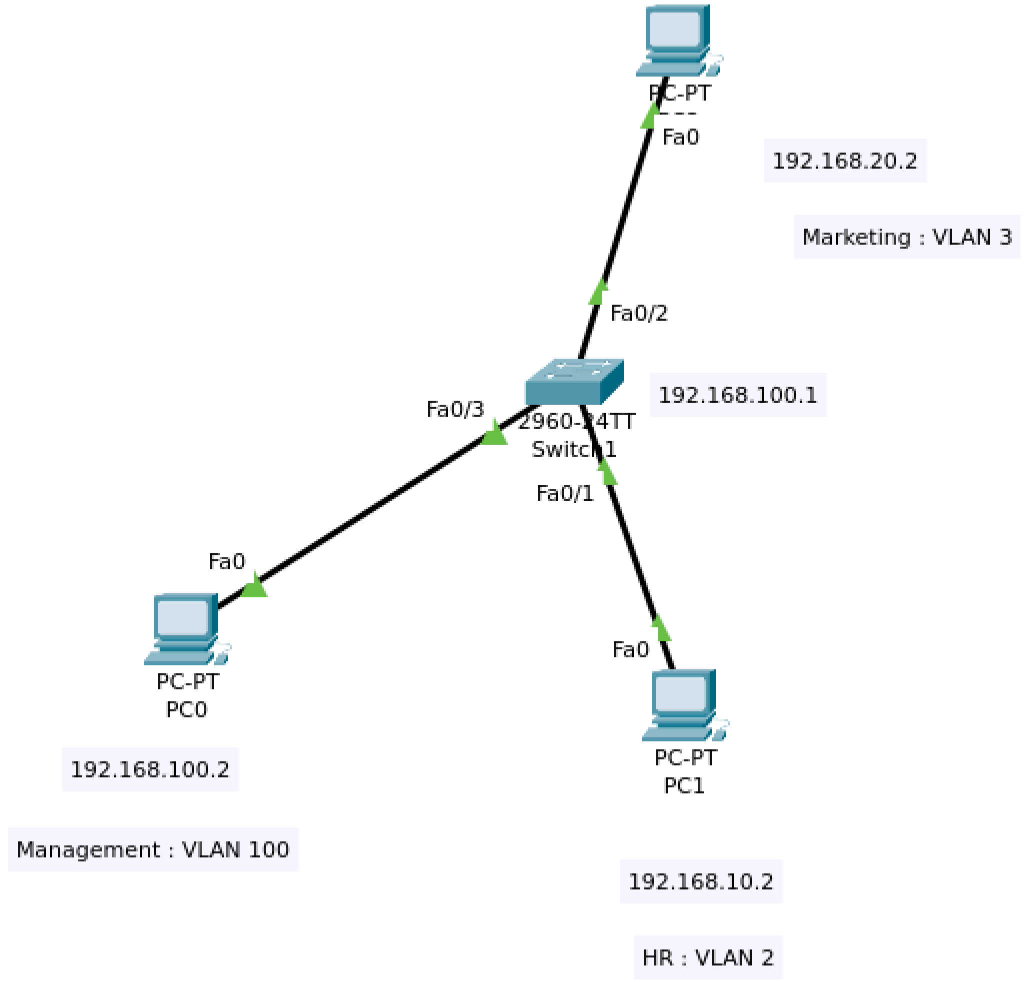
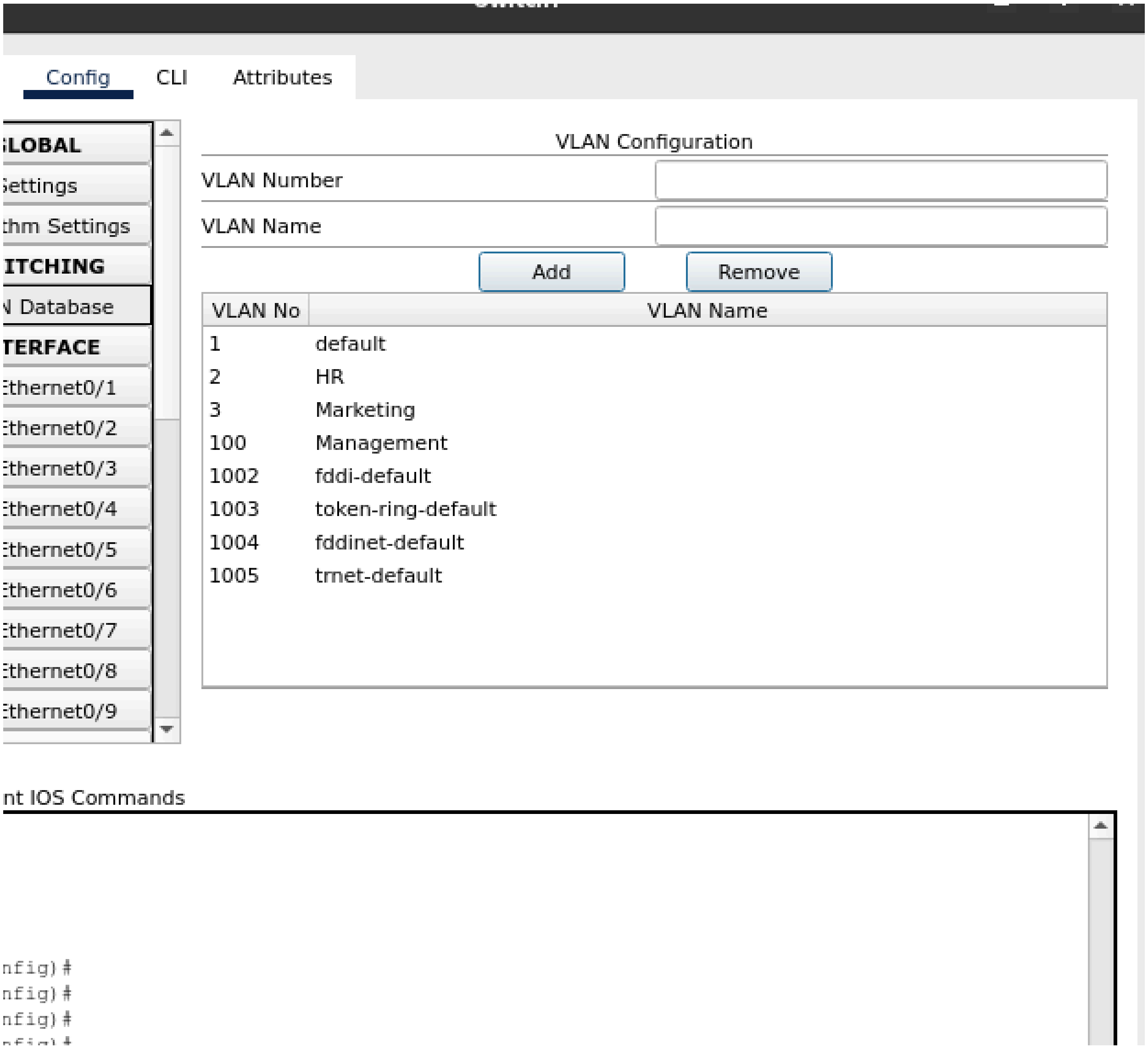
Name: J Kevin Immanuel
College: VIT Chennai

Q7)



For this, I will be using 3 VLANS : HR, Marketing and Management and only Management will be able to ssh into the switch.

First, i will configure the VLANs



VLAN Configuration

VLAN Number

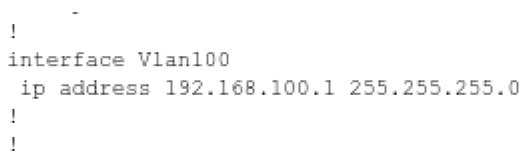
VLAN Name

VLAN No	VLAN Name
1	default
2	HR
3	Marketing
100	Management
1002	fddi-default
1003	token-ring-default
1004	fddinet-default
1005	trnet-default

nt IOS Commands

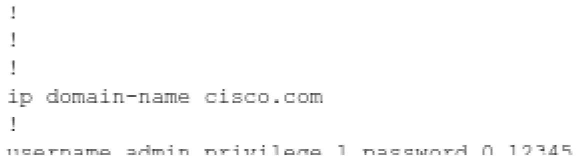
```
nfig)#
nfig)#
nfig)#
```

Next, I will set an IP to the Switch with the interface VLAN 100 (Management). This IP will be so that only Management can access and not any other device.



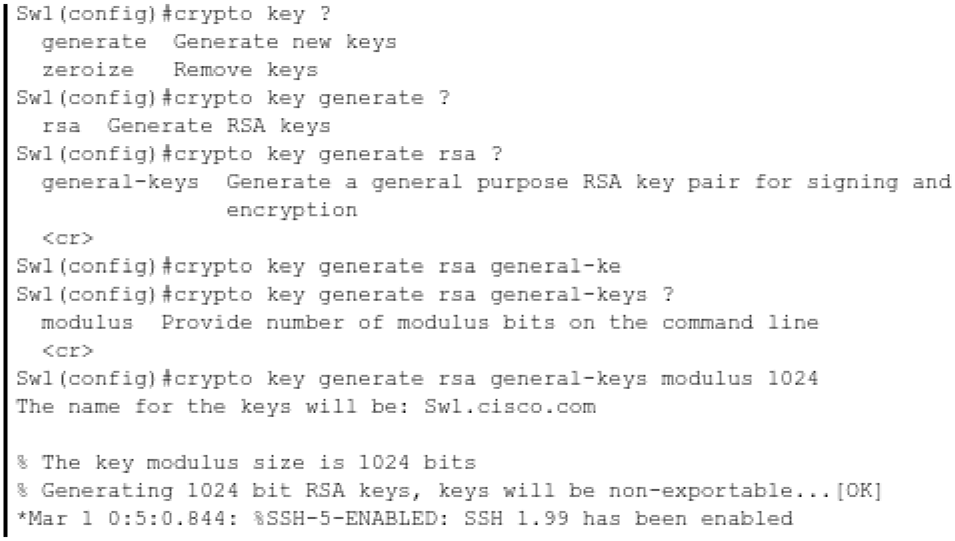
```
!
interface Vlan100
 ip address 192.168.100.1 255.255.255.0
!
!
```

Next, I will assign a domain name:



```
!
!
!
ip domain-name cisco.com
!
username admin privilege 1 password 0 12345
```

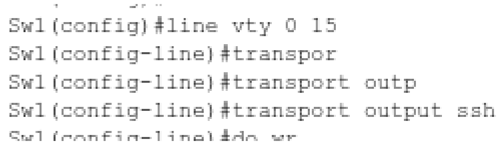
After this, we will generate crypto keys which enables ssh:



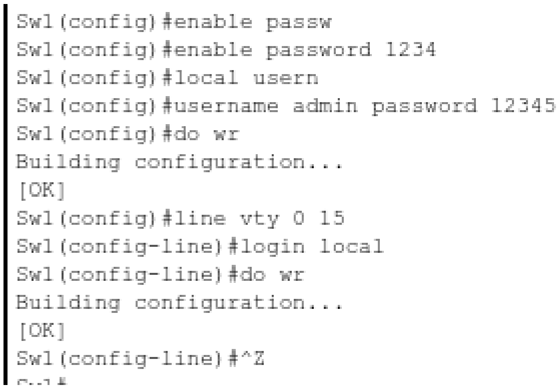
```
Sw1(config)#crypto key ?
  generate  Generate new keys
  zeroize   Remove keys
Sw1(config)#crypto key generate ?
  rsa  Generate RSA keys
Sw1(config)#crypto key generate rsa ?
  general-keys  Generate a general purpose RSA key pair for signing and
                encryption
  <cr>
Sw1(config)#crypto key generate rsa general-ke
Sw1(config)#crypto key generate rsa general-keys ?
  modulus  Provide number of modulus bits on the command line
  <cr>
Sw1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: Sw1.cisco.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:5:0.844: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Next, we will enable ssh sessions, along with creating a Switch enable password, a local user and password:



```
Sw1(config)#line vty 0 15
Sw1(config-line)#transpor
Sw1(config-line)#transport outp
Sw1(config-line)#transport output ssh
Sw1(config-line)#do wr
```

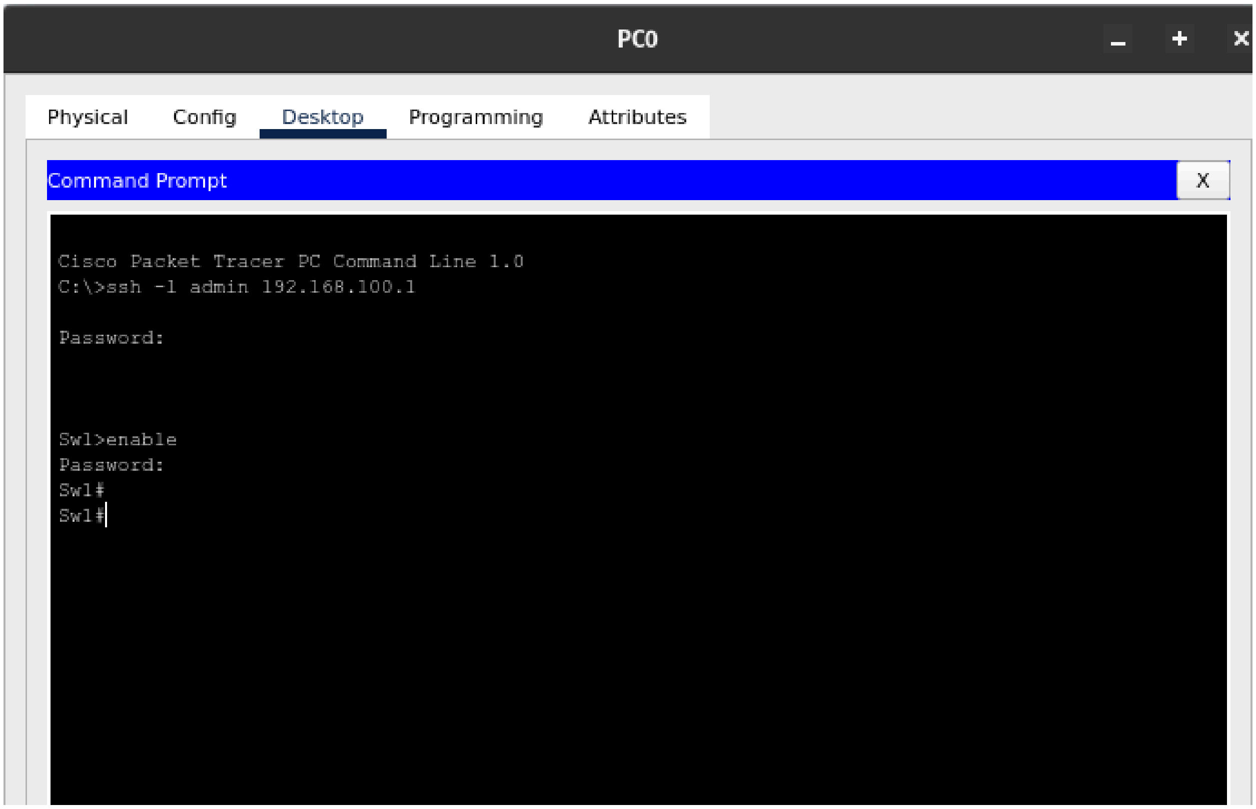


```
Sw1(config)#enable passw
Sw1(config)#enable password 1234
Sw1(config)#local usern
Sw1(config)#username admin password 12345
Sw1(config)#do wr
Building configuration...
[OK]
Sw1(config)#line vty 0 15
Sw1(config-line)#login local
Sw1(config-line)#do wr
Building configuration...
[OK]
Sw1(config-line)#^Z
Sw1#
```

This tells the switch to login using local account when someone ssh into the switch.

Now, we can successfully ssh into the switch.

Management PC:



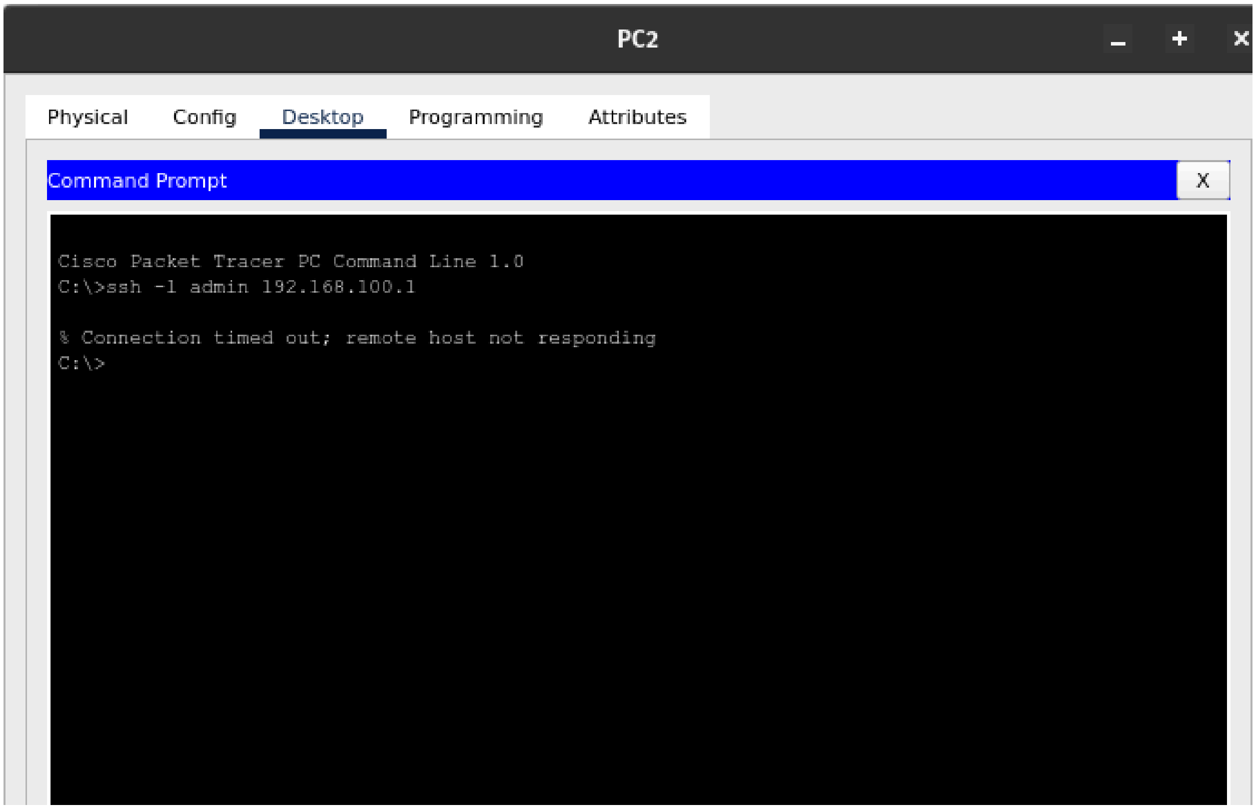
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 192.168.100.1

Password:



Sw1>enable
Password:
Sw1#
Sw1#
```

HR PC:



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 192.168.100.1

% Connection timed out; remote host not responding
C:\>
```

Thus, we can see that we can only ssh using the management PC and not any other VLAN pc.