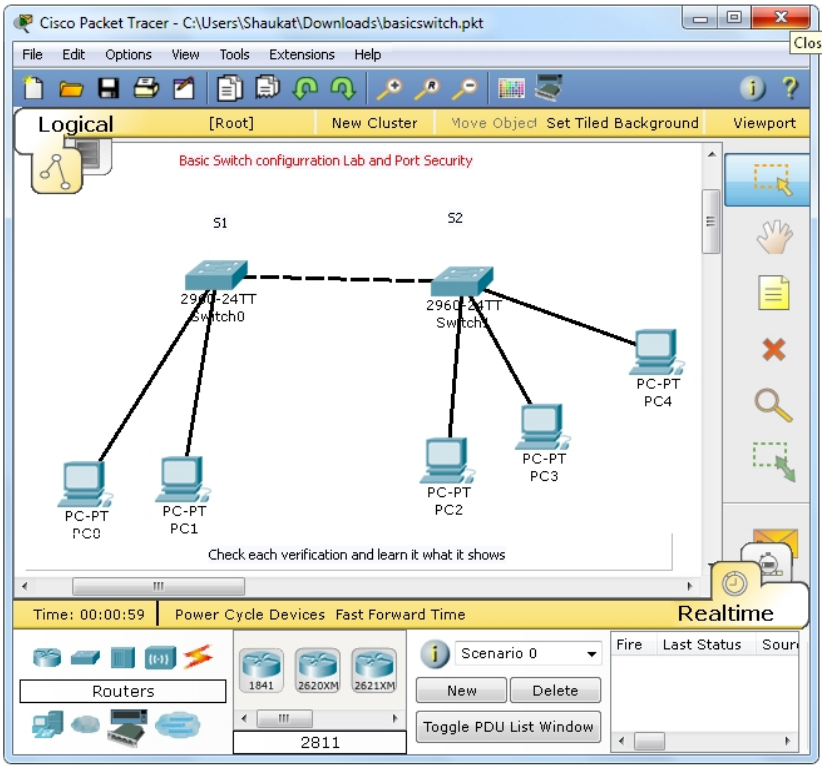

Switch Configuration

1- set host name on switch S1
Switch>enable
Switch#configure terminal
Switch(config)#hostname S1

2- set Console password or usermode password
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit

3- set privilige mode password
S1(config)#enable secret class

4- All password should be encrypted
S1(config)#service password-encryption

5- set banner motd
S1(config)#banner motd # Maintinance will be occured on friday #

6- set terminal history size 50

S1(config)#exit
S1#terminal history size 50

7- set interface speed and duplex setting auto on interface fa0/1
S1(config)#interface fa0/1
S1(config-if)#speed auto
S1(config-if)#duplex auto

8- set ip address on interface VLAN 1
S1(config-if)#exit
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.254 255.255.255.0
S1(config-if)#no shutdown

9- enabel telnet on switch for Remote access
S1(config-if)#exit
S1(config)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit

10- S1 configuration Verification

```
S1#show running-config
S1#show ip interface brief
S1#show interface
S1#show interface fa0/1
```

11- Set ip address on Host

Pc0= 192.168.1.1
Pc1= 192.168.1.2
Pc2= 192.168.1.3
Pc4=192.168.1.4

12- Ping from Pc2 to Pc0,Pc1

In command prompt type
Ping 192.168.1.1

13- Remote Access switch S1 from Pc0

In command Prompt type
telnet 192.168.1.254

14- Port security on S1 (configure port fa0/1 to maximum allow 3 pc or 3 mac address using
a sticky mac-address command)if it exceded then violation mode set to protect.

```
S1(config)#int fa0/1
 S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
 S1(config-if)#switchport port-security ?
  mac-address  Secure mac address
  maximum      Max secure addresses
  violation    Security violation mode
S1(config-if)#switchport port-security maximum 3
 S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#switchport port-security violation ?
 protect   Security violation protect mode
```

```
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
```

```
S1(config-if)#switchport port-security violation protect
S1(config-if)#exit
```

15- Verification of port security and mac address

```
S1#show port-security
S1#show port-security interface fastEthernet 0/1
S1#show mac-address-table
S1#show interface fa0/1
S1#show arp
S1#show running-config
```

16- Repeat step 12 and check mac address table and port security

17 - add another PC on S2 and set ip address 192.168.1.5 and ping to pc0
packet should be failed

18- enable SSH on switch S1

```
S1(config)#ip domain-name cisco.com
S1(config)#ip ssh version 2
S1(config)#crypto key generate rsa
How many bits in the modulus [512]: (set 1024 and Enter)
S1(config)#line vty 0 4
S1(config-line)#transport input ?
  all     All protocols
  none    No protocols
  ssh     TCP/IP SSH protocol
  telnet  TCP/IP Telnet protocol
S1(config-line)#transport input ssh
Create Username and Password for SSH access
S1(config)#username cisco privilege 15 secret cisco
```

19- Remote access Switch S1 from Pc0 using telnet and ssh and check status
For ssh access type on command prompt
PC>ssh -l cisco 192.168.1.254 and enter

and you must need to save all configuration on S1

S1#copy running-config startup-config
for Remote backup
S1#copy running-config tftp:

Some Useful Commands (Please do not apply in your lab)

i) erase nvram or startup configuration
S1#erase startup-config
ii) Delete Operationg system or Flash

S1#delete flash:

iii) Set default gateway on Switch How to access from another network
S1(config)#ip default-gateway 192.168.1.253
where 253 is router ip address