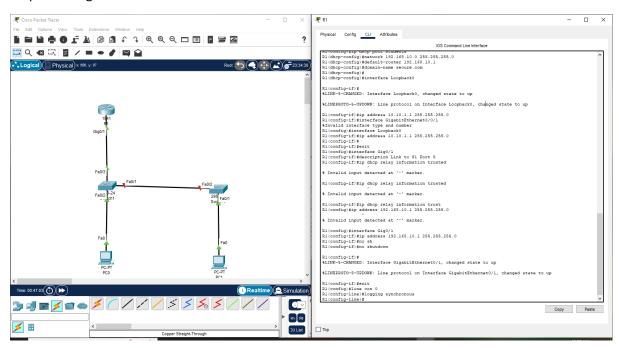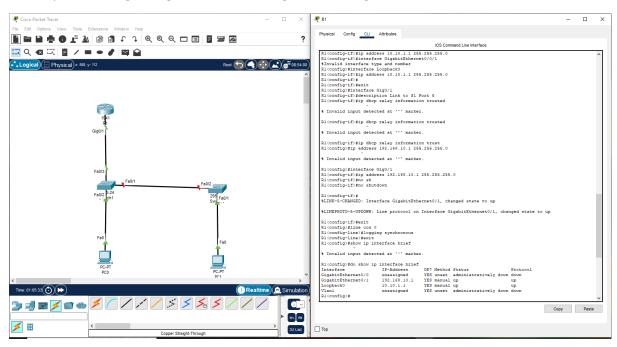# Packet Tracer Lab: Switch Security Configuration

Step 1: Cable the network.
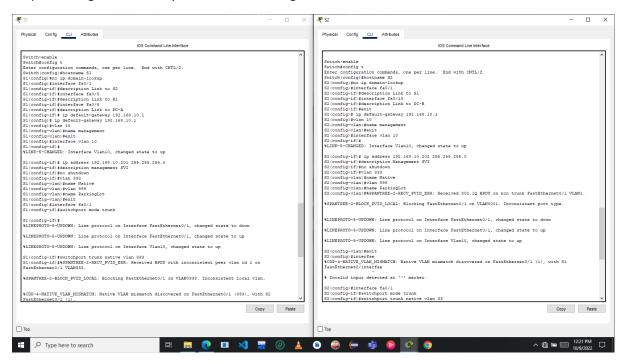
Step 2: Configure R1.

2. Verify the running-configuration on R1 using the following command:
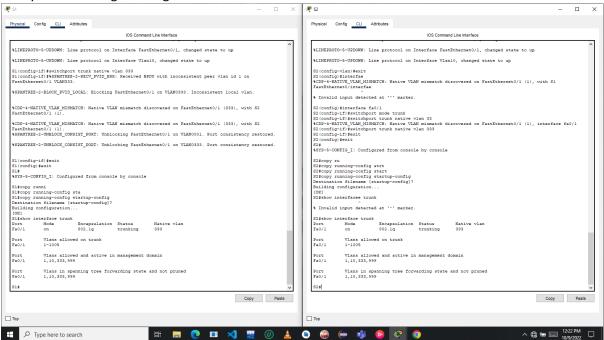
Step 3: Configure and verify basic switch settings.

S1 — IOS Command Line Interface
```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#interface fa0/1
S1(config-if)#description Link to S2
S1(config-if)#interface fa0/5
S1(config-if)#description Link to R1
S1(config-if)#interface fa0/6
S1(config-if)#description Link to PC-A
S1(config-if)# ip default-gateway 192.168.10.1
S1(config-if)# ip default-gateway 192.168.10.1
S1(config)#vlan 10
S1(config-vlan)#name management
S1(config-vlan)#exit
S1(config)#interface vlan 10
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

S1(config-if)# ip address 192.168.10.201 255.255.255.0
S1(config-if)#description management SVI
S1(config-if)#no shutdown
S1(config-if)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#vlan 999
S1(config-vlan)#name ParkingLot
S1(config-vlan)#exit
S1(config)#interface fa0/1
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

S1(config-if)#switchport trunk native vlan 333
S1(config-if)#$SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 1 on
FastEthernet0/1 VLAN333.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0333. Inconsistent local vlan.

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (333), with S2
FastEthernet0/1 (1).
```

S2 — IOS Command Line Interface
```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#interface fa0/1
S2(config-if)#description Link to S1
S2(config-if)#interface fa0/18
S2(config-if)#description Link to PC-B
S2(config-if)#exit
S2(config)# ip default-gateway 192.168.10.1
S2(config)#vlan 10
S2(config-vlan)#name management
S2(config-vlan)#exit
S2(config)#interface vlan 10
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

S2(config-if)# ip address 192.168.10.202 255.255.255.0
S2(config-if)#description Management SVI
S2(config-if)#no shutdown
S2(config-if)#vlan 333
S2(config-vlan)#name Native
S2(config-vlan)#vlan 999
S2(config-vlan)#name ParkingLot
S2(config-vlan)#$SPANTREE-2-RECV_PVID_ERR: Received 802.1Q BPDU on non trunk FastEthernet0/1 VLAN1.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0001. Inconsistent port type.

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

S2(config-vlan)#exit
S2(config)#interfae
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with S1
FastEthernet0/interfae
          ^
% Invalid input detected at '^' marker.

S2(config)#interface fa0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 33
```

Part 2: Configure VLANs on Switches.

Part 3: Configure Switch Security.

Step 1: Implement 802.1Q trunking.

Verify that trunking is configured on both switches.

S1 — IOS Command Line Interface
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

S1(config-if)#switchport trunk native vlan 333
S1(config-if)#$SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 1 on
FastEthernet0/1 VLAN333.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0333. Inconsistent local vlan.

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (333), with S2
FastEthernet0/1 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (333), with S2
FastEthernet0/1 (1).
%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0001. Port consistency restored.

%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0333. Port consistency restored.

S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy runni
S1#copy running-config sta
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#show interface trunk
Port       Mode         Encapsulation  Status        Native vlan
Fa0/1      on           802.1q         trunking      333

Port       Vlans allowed on trunk
Fa0/1      1-1005

Port       Vlans allowed and active in management domain
Fa0/1      1,10,333,999

Port       Vlans in spanning tree forwarding state and not pruned
Fa0/1      1,10,333,999

S1#
```

S2 — IOS Command Line Interface
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

S2(config-vlan)#exit
S2(config)#interfae
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with S1
FastEthernet0/interfae
          ^
% Invalid input detected at '^' marker.

S2(config)#interface fa0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 33
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), interface fa0/1
S2(config-if)#switchport trunk native vlan 333
S2(config-if)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#copy ru
S2#copy running-config strt
S2#copy running-config start
S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S2#show interfacee trunk
          ^
% Invalid input detected at '^' marker.

S2#show interface trunk
Port       Mode         Encapsulation  Status        Native vlan
Fa0/1      on           802.1q         trunking      333

Port       Vlans allowed on trunk
Fa0/1      1-1005

Port       Vlans allowed and active in management domain
Fa0/1      1,10,333,999

Port       Vlans in spanning tree forwarding state and not pruned
Fa0/1      1,10,333,999

S2#
```

Step 2: Configure access ports.

Step 3: Secure and disable unused switchports.

Verify that unused ports are disabled and associated with VLAN 999 by issuing the show command.

S2 — IOS Command Line Interface

```
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
S2(config-if-range)#
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/15, changed state to down

S2(config-if-range)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#copy ru
S2#copy running-config
S2#copy running-config star
S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S2#show interface status
Port    Name            Status      Vlan    Duplex  Speed Type
Fa0/1   Link to S1      connected   trunk   auto    auto 10/100BaseTX
Fa0/2                   disabled 999 auto    auto 10/100BaseTX
Fa0/3                   disabled 999 auto    auto 10/100BaseTX
Fa0/4                   disabled 999 auto    auto 10/100BaseTX
Fa0/5                   disabled 999 auto    auto 10/100BaseTX
Fa0/6                   disabled 999 auto    auto 10/100BaseTX
Fa0/7                   disabled 999 auto    auto 10/100BaseTX
Fa0/8                   disabled 999 auto    auto 10/100BaseTX
Fa0/9                   disabled 999 auto    auto 10/100BaseTX
Fa0/10                  disabled 999 auto    auto 10/100BaseTX
Fa0/11                  disabled 999 auto    auto 10/100BaseTX
Fa0/12                  disabled 999 auto    auto 10/100BaseTX
Fa0/13                  disabled 999 auto    auto 10/100BaseTX
Fa0/14                  disabled 999 auto    auto 10/100BaseTX
Fa0/15                  disabled 999 auto    auto 10/100BaseTX
Fa0/16                  disabled 999 auto    auto 10/100BaseTX
Fa0/17                  disabled 999 auto    auto 10/100BaseTX
Fa0/18  Link to PC-B    notconnect  10      auto    auto 10/100BaseTX
Fa0/19                  disabled 999 auto    auto 10/100BaseTX
Fa0/20                  disabled 999 auto    auto 10/100BaseTX
Fa0/21                  disabled 999 auto    auto 10/100BaseTX
--More--
```

S1 — IOS Command Line Interface

```
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
S1(config-if-range)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy runn
S1#copy running-config star
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#show interfaces status
Port    Name            Status      Vlan    Duplex  Speed Type
Fa0/1   Link to S2      connected   trunk   auto    auto 10/100BaseTX
Fa0/2                   disabled 999 auto    auto 10/100BaseTX
Fa0/3                   disabled 999 auto    auto 10/100BaseTX
Fa0/4                   disabled 999 auto    auto 10/100BaseTX
Fa0/5   Link to R1      connected   10      auto    auto 10/100BaseTX
Fa0/6   Link to PC-A    connected   10      auto    auto 10/100BaseTX
Fa0/7                   disabled 999 auto    auto 10/100BaseTX
Fa0/8                   disabled 999 auto    auto 10/100BaseTX
Fa0/9                   disabled 999 auto    auto 10/100BaseTX
Fa0/10                  disabled 999 auto    auto 10/100BaseTX
Fa0/11                  disabled 999 auto    auto 10/100BaseTX
Fa0/12                  disabled 999 auto    auto 10/100BaseTX
Fa0/13                  disabled 999 auto    auto 10/100BaseTX
Fa0/14                  disabled 999 auto    auto 10/100BaseTX
Fa0/15                  disabled 999 auto    auto 10/100BaseTX
Fa0/16                  disabled 999 auto    auto 10/100BaseTX
Fa0/17                  disabled 999 auto    auto 10/100BaseTX
Fa0/18                  disabled 999 auto    auto 10/100BaseTX
Fa0/19                  disabled 999 auto    auto 10/100BaseTX
Fa0/20                  disabled 999 auto    auto 10/100BaseTX
Fa0/21                  disabled 999 auto    auto 10/100BaseTX
--More--
```

Step 4: Document and implement port security features.

Verify port security on S1 F0/6.

Verify port security on S2 F0/18

S2 — IOS Command Line Interface

```
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface fa0/18
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#exit
S2(config)#interface fa0/18
S2(config-if)# switchport port-security aging time 60
S2(config-if)#switchport port-security maximum 2
S2(config-if)#switchport port-security violation protect
S2(config-if)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#copy run
S2#copy running-config sta
S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S2#show port-security interface f0/18
Port Security                : Enabled
Port Status                  : Secure-down
Violation Mode               : Protect
Aging Time                   : 60 mins
Aging Type                   : Absolute
SecureStatic Address Aging   : Disabled
Maximum MAC Addresses        : 2
Total MAC Addresses          : 0
Configured MAC Addresses     : 0
Sticky MAC Addresses         : 0
Last Source Address:Vlan     : 0000.0000.0000:0
Security Violation Count     : 0

S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)# ip dhcp snooping
S2(config)# ip dhcp snooping vlan 10
S2(config)#interface f0/1
S2(config-if)# ip dhcp snooping trust
S2(config-if)#exit
S2(config)#interface f0/18
S2(config-if)#ip dhcp snooping limit rate 5
S2(config-if)#exit
S2(config)#exit
S2#
```

S1 — IOS Command Line Interface

```
% Invalid input detected at '^' marker.

S1(config-if)#switchport port-security aging inactivity
                                         ^
% Invalid input detected at '^' marker.

S1(config-if)#switchport port-security agin
S1(config-if)#switchport port-security aging help
                                              ^
% Invalid input detected at '^' marker.

S1(config-if)#switchport port-security aging -h
                                             ^
% Invalid input detected at '^' marker.

S1(config-if)#help
               ^
% Invalid input detected at '^' marker.

S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
cop
% Incomplete command.
S1#copy runnin
S1#copy running-config st
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#show port-security interface fa0/6
Port Security                : Enabled
Port Status                  : Secure-up
Violation Mode               : Restrict
Aging Time                   : 60 mins
Aging Type                   : Absolute
SecureStatic Address Aging   : Disabled
Maximum MAC Addresses        : 3
Total MAC Addresses          : 0
Configured MAC Addresses     : 0
Sticky MAC Addresses         : 0
Last Source Address:Vlan     : 0000.0000.0000:0
Security Violation Count     : 0

S1#
```
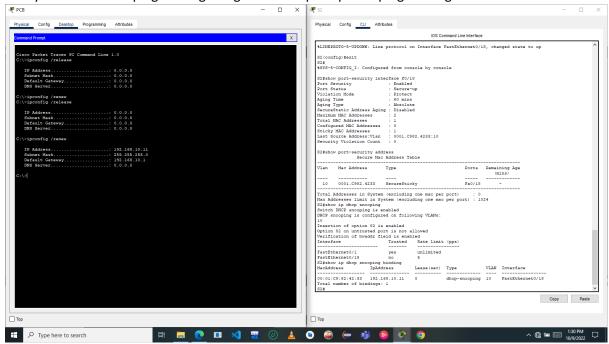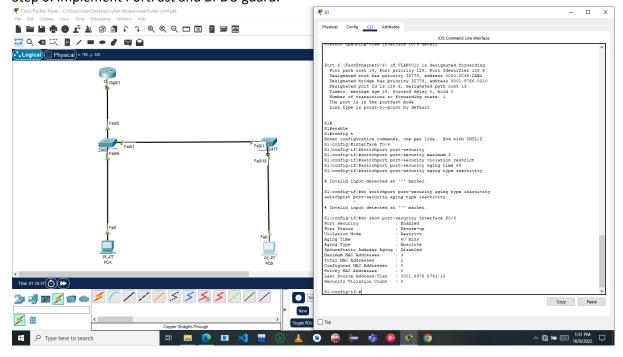
Step 5: Implement DHCP snooping security.

Verify DHCP Snooping on S2.

From the command prompt on PC-B, release and then renew the IP address.

Verify the DHCP snooping binding using the show ip dhcp snooping binding command.

Step 6: Implement PortFast and BPDU guard.

Step 7: Verify end-to-end connectivity.