

VLANs and Secure Switch Configuration

Introduction

A Virtual Local Area Network (VLAN) is a way of logically dividing a physical LAN into multiple separate virtual networks that are broadcast domains. For example, we could have a network that is separate for guests or specific departments. The segmentation is done through software on a network switch. The segmentation allows devices to communicate as if they were on the same physical LAN, even if they are connected to different switches or in different physical locations. There is also traffic isolation provided by the VLANs; a broadcast frame sent within one VLAN is only seen by devices in that same VLAN, not by devices in other VLANs. Thus VLANs are used to improve security, network traffic management, and network administration.

VLANs are one of Layer 2's security features. Others include **port security** (limits the number of MAC addresses allowed on a switch port), **DHCP snooping** (prevents unauthorized DHCP servers from assigning IP addresses), and **dynamic ARP inspection** (validates ARP packets to prevent spoofing).

This lab aims to review previously covered Layer 2 security features while also covering switch security configuration.

Objectives

Part 1: Configure the Network Devices.

- Cable the network.
- Configure R1.
- Configure and verify basic switch settings.

Part 2: Configure VLANs on Switches.

- Configure VLAN 10.
- Configure the SVI for VLAN 10.
- Configure VLAN 333 with the name Native on S1 and S2.

-
- Configure VLAN 999 with the name ParkingLot on S1 and S2.

Part 3: Configure Switch Security.

- Implement 802.1Q trunking.
- Configure access ports.
- Secure and disable unused switchports.
- Document and implement port security features.
- Implement DHCP snooping security.
- Implement PortFast and BPDU guard.
- Verify end-to-end-connectivity.

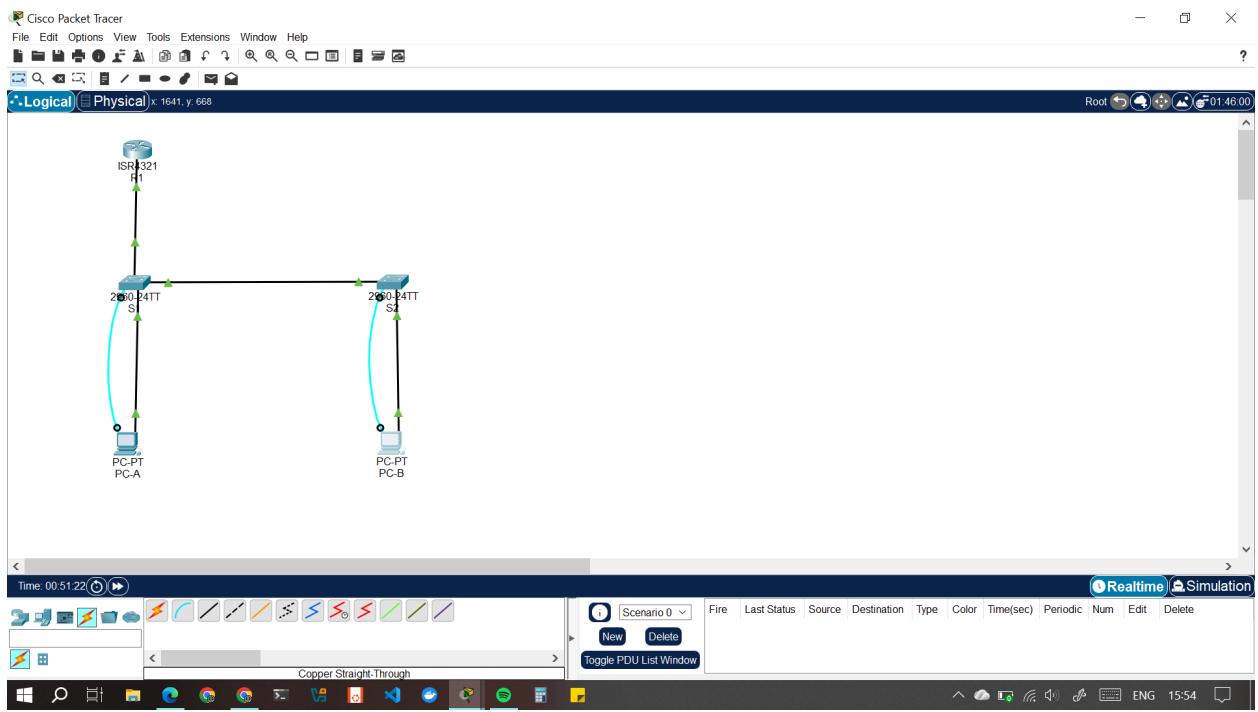
Required Resources

- 1 Router (Cisco 4221 with Cisco IOS XE Release 16.9.3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows with a terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Configure the Network Devices.

Step 1: Cable the network.

1. Cable the network as shown in the topology.
2. Initialize the devices.



Step 2: Configure R1.

1. Load the following configuration script on R1.

```
enable
```

```
configure terminal
```

```
hostname R1
```

```
no ip domain lookup
```

```
ip dhcp excluded-address 192.168.10.1 192.168.10.9
```

```
ip dhcp excluded-address 192.168.10.201 192.168.10.202
```

```
!
```

```
ip dhcp pool Students
```

```
network 192.168.10.0 255.255.255.0
```

```
default-router 192.168.10.1

domain-name secure.com

!

interface Loopback0

ip address 10.10.1.1 255.255.255.0

!

interface GigabitEthernet0/0/1

description Link to S1 Port 5

ip dhcp relay information trusted

ip address 192.168.10.1 255.255.255.0

no shutdown

!

line con 0

logging synchronous

exec-timeout 0 0
```

2. Verify the running-configuration on R1 using the following command: **show ip interface brief**

```

R1# 
R1(config)#ip dhcp excluded-address 192.168.10.201 192.168.10.202
R1(config)#ip dhcp pool Students
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.10.1
R1(dhcp-config)#domain-name secure.com
R1(dhcp-config)#exit
R1(config)#interface Loopback0
R1(config-if)#ip address 10.10.1.1 255.255.255.0
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R1(config-if)#exit
R1(config)#interface GigabitEthernet0/0/1
R1(config-if)#description Link to S1 Port 5
R1(config-if)#ip dhcp relay information trusted
^
% Invalid input detected at '^' marker.
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#shutdown
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
R1(config-if)#exit
R1(config)#line con 0
R1(config-line)#logging synchronous
R1(config-line)#exec-timeout 0 0
R1(config-line)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#show ip interface brief
Interface          IP-Address      OK? Method Status        Protocol
GigabitEthernet0/0/0  unassigned     YES unset administratively down    down
GigabitEthernet0/0/1  192.168.10.1  YES manual up         up
Loopback0            10.10.1.1    YES manual up         up
Vlan1               unassigned     YES unset administratively down    down
R1#

```

3. Verify IP addressing and interfaces are in an up / up state (troubleshoot as necessary).

Step 3: Configure and verify basic switch settings.

1. Configure the hostname for switches S1 and S2.
2. Prevent unwanted DNS lookups on both switches.
3. Configure interface descriptions for the ports that are in use in S1 and S2.
4. Set the default-gateway for the Management VLAN to 192.168.10.1 on both switches.

S2

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Switch con0 is now available

Press RETURN to get started.

Switch>config t
^
% Invalid input detected at '^' marker.

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)#ip domain-list lookup
S2(config)#interface f0/1
S2(config-if)#description Link to S1
S2(config-if)#interface f0/18
S2(config-if)#description Link to PC-B
S2(config-if)# ip default-gateway 192.168.10.1]
S2(config-if)# ip default-gateway 192.168.10.1
S2(config)#

```

Top

Copy Paste

S1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Switch con0 is now available

Press RETURN to get started.

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

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 f0/1
S1(config-if)#description Link to S2
S1(config-if)#interface f0/5
S1(config-if)#description Link to R1
S1(config-if)#interface f0/6
S1(config-if)#description Link to PC-A
S1(config-if)# ip default-gateway 192.168.10.1
S1(config)# no ip domain-lookup
S1(config)#

```

Top

Copy Paste

Part 2: Configure VLANs on Switches.

Step 1: Configure VLAN 10.

1. Add VLAN 10 to S1 and S2 and name the VLAN Management.

S1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Switch con0 is now available

Press RETURN to get started.

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

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 f0/1
S1(config-if)#description Link to S2
S1(config-if)#interface f0/5
S1(config-if)#description Link to R1
S1(config-if)#interface f0/6
S1(config-if)#description Link to PC-A
S1(config-if)#ip default-gateway 192.168.10.1
S1(config)#no ip domain-lookup
S1(config)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#

```

Top

Copy Paste



S2

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Switch con0 is now available

Press RETURN to get started.

Switch>config t
^
% Invalid input detected at '^' marker.

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)#no ip domain-lookup
S2(config)#interface f0/1
S2(config-if)#description Link to S1
S2(config-if)#interface f0/18
S2(config-if)#description Link to PC-B
S2(config-if)#ip default-gateway 192.168.10.1
S2(config-if)#ip default-gateway 192.168.10.1
S2(config)#vlan 10
S2(config-vlan)#name Management
S2(config-vlan)#

```

Top

Copy Paste



Step 2: Configure the SVI for VLAN 10.

2. Configure the IP address according to the Addressing Table for SVI for VLAN 10 on S1 and S2. Enable the SVI interfaces and provide a description for the interface.

S1

```

S1(config-if)#ip default-gateway 192.168.10.1
S1(config)#no ip domain-lookup
S1(config)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#
S1 con0 is now available

Press RETURN to get started.

S1>enable
S1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
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)#exit

```

Top Copy Paste

S2

```

S2#exit
S2 con0 is now available

Press RETURN to get started.

S2>configure t
% Invalid input detected at '^' marker.
S2#enable
S2#configure t
Enter configuration commands, one per line. End with CNTL/Z.
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

```

Top Copy Paste

Step 3: Configure VLAN 333 with the name Native on S1 and S2.

Step 4: Configure VLAN 999 with the name ParkingLot on S1 and S2.

```
S1(config-vlan)# vlan 999
```

```
S1(config-vlan)# name ParkingLot
```

```
S2(config-vlan)# vlan 999
```

```
S2(config-vlan)# name ParkingLot
```

S1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
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)#exit
S1(config)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#
S1 con0 is now available

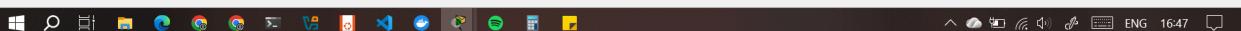
Press RETURN to get started.

S1>enable
S1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#vlan 999
S1(config-vlan)#name ParkingLot
S1(config-vlan)#exit
S1(config)#

```

Top

Copy Paste



S2

Physical Config **CLI** Attributes

IOS Command Line Interface

```
%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)#
S2 con0 is now available

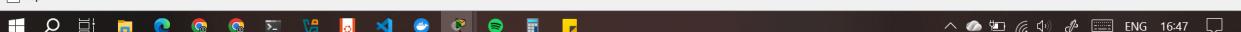
Press RETURN to get started.

S2>enable
S2#configure t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#vlan 333
S2(config-vlan)#name Native
S2(config-vlan)#vlan 999
S2(config-vlan)#name ParkingLot
S2(config-vlan)#

```

Top

Copy Paste



Part 3: Configure Switch Security.

Step 1: Implement 802.1Q trunking.

1. On both switches, configure trunking on F0/1 to use VLAN 333 as the native VLAN.
2. Verify that trunking is configured on both switches.

S1

```

Physical Config CLI Attributes
IOS Command Line Interface

      Fa0/14, Fa0/15, Fa0/16, Fa0/17
      Fa0/18, Fa0/19, Fa0/20, Fa0/21
      Fa0/22, Fa0/23, Fa0/24, Gig0/1
      Gig0/2

10 Management          active
333 Native            active
999 ParkingLot        active
1002 fddi-default     active
1003 token-ring-default active
1004 ethernet-default active
1005 tracet-default   active
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#spanning-tree vlan 1,10,333,999 priority 4096
S1(config)#end
S1#
$SYS-5-CONFIG_I: Configured from console by console

S1#
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to down
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%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#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#

```

Top

Copy Paste

S2

```

Physical Config CLI Attributes
IOS Command Line Interface

S2>show spanning-tree brief
^
% Invalid input detected at '^' marker.

S2>enable
S2#show interfaces 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#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##

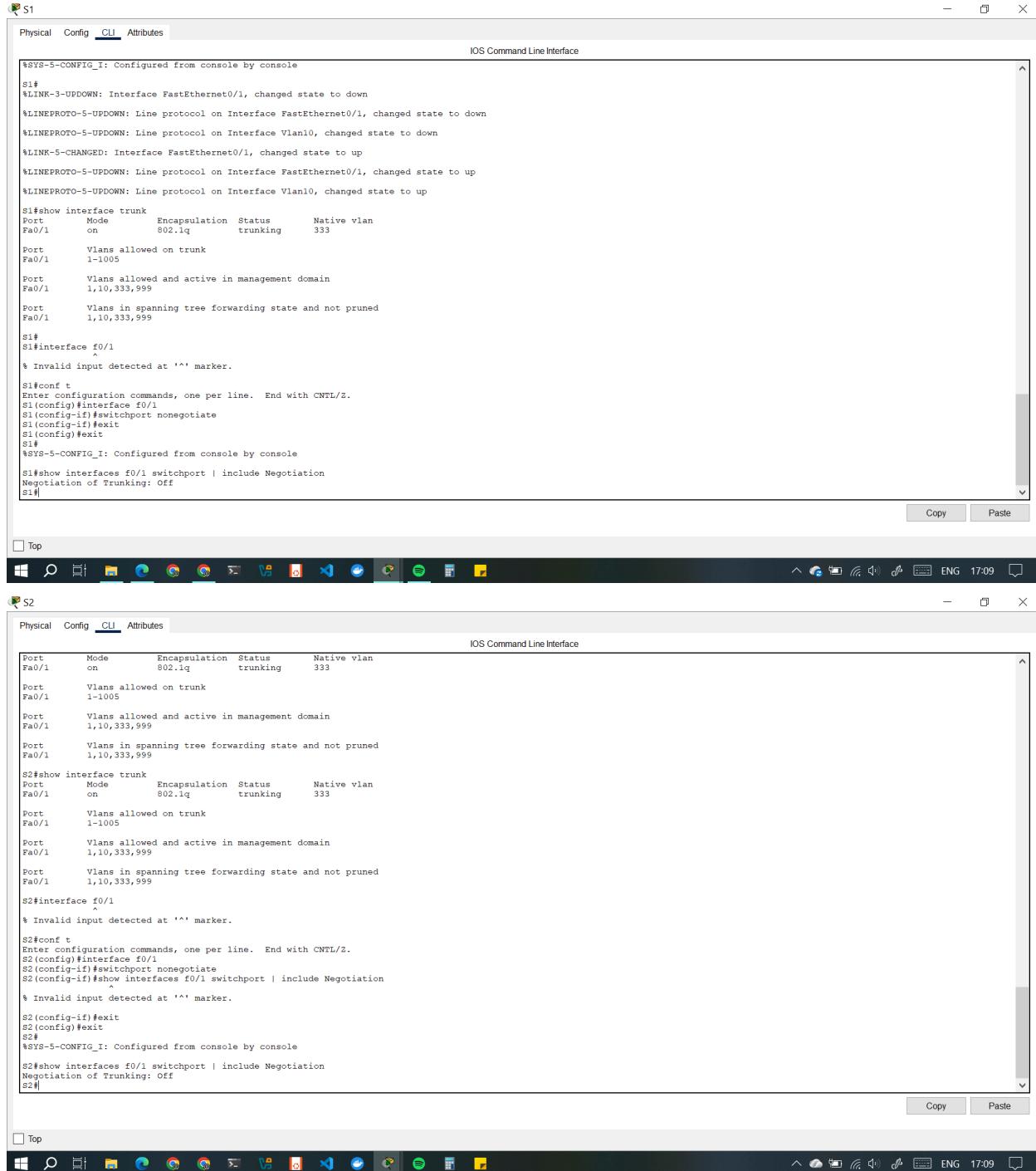
```

Top

Copy Paste

3. Disable DTP negotiation on F0/1 on S1 and S2.

4. Verify with the show interfaces command.



S1

```
$SYS-5-CONFIG_I: Configured from console by console
S1#
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to down
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%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#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#
S1#interface f0/1
^
% Invalid input detected at '^' marker.

S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface F0/1
S1(config-if)#switchport nonegotiate
S1(config-if)#exit
S1(config)#exit
S1#
$SYS-5-CONFIG_I: Configured from console by console
S1#show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
S1#
```

Copy Paste

Top

S2

```
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#show interface f0/1
^
% Invalid input detected at '^' marker.

S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface F0/1
S2(config-if)#switchport nonegotiate
S2(config-if)#show interfaces f0/1 switchport | include Negotiation
^
% Invalid input detected at '^' marker.

S2(config-if)#exit
S2(config)#exit
S2#
$SYS-5-CONFIG_I: Configured from console by console
S2#show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
S2#
```

Copy Paste

Top

Step 2: Configure access ports.

1. On S1, configure F0/5 and F0/6 as access ports that are associated with VLAN 10.
2. On S2, configure F0/18 as an access port that is associated with VLAN 10.

S2

Physical Config **CLI** Attributes

IOS Command Line Interface

```

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

S2#show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
S2#

S2 con0 is now available

Press RETURN to get started.

S2>enable
S2>config
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#

```

Top

Copy Paste

S1

Physical Config **CLI** Attributes

IOS Command Line Interface

```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
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    1,10,33,999
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    1,10,33,999
S1#
S1#interface f0/1
% Invalid input detected at '^' marker.

S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface f0/1
S1(config-if)#switchport nonegotiate
S1(config-if)#exit
S1(config)#exit
S1#
$SYS-5-CONFIG_I: Configured from console by console

S1#show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
S1#interface range f0/5 6
S1#interface range f0/5 - 6
% Invalid input detected at '^' marker.

S1(config)interface range f0/5 - 6
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 10
S1(config-if-range)#

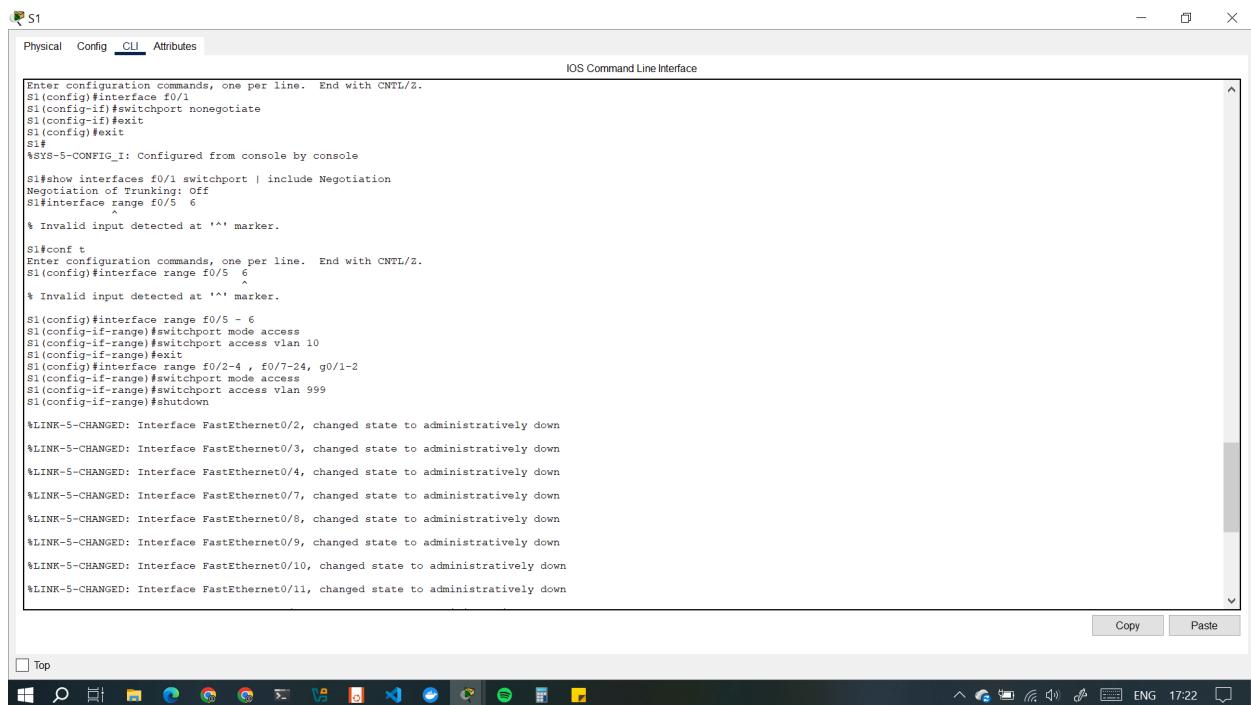
```

Top

Copy Paste

Step 3: Secure and disable unused switchports.

1. On S1 and S2, move the unused ports from VLAN 1 to VLAN 999 and disable the unused ports.
2. Verify that unused ports are disabled and associated with VLAN 999 by issuing the show command.



```
S1
Physical Config CLI Attributes
IOS Command Line Interface

Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface f0/1
S1(config-if)#switchport nonegotiate
S1(config-if)#exit
S1(config)#exit
S1
%SYS-5-CONFIG_I: Configured from console by console

S1#show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: off
S1#interface range f0/5 6
^
% Invalid input detected at '^' marker.

S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface range f0/5 6
^
% Invalid input detected at '^' marker.

S1(config)#interface range f0/5 6
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 10
S1(config-if-range)#exit
S1(config)#interface range f0/2-4, f0/7-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 999
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down
```

S2

Physical Config **CLI** Attributes

IOS Command Line Interface

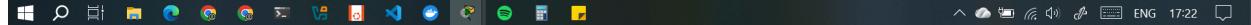
Press RETURN to get started.

```
S2>enable
S2>conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#exit
S2(config)#interface range f0/2-17, f0/19-24, g0/1-2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 999
S2(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
```

Top

Copy Paste



S2

```
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
%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
S2(config-if-range)#exit
S2(config)#exit
S2#
$SYS-5-CONFIG_I: Configured from console by console

S2#show interfaces 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 connected 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-->
```

Top

Copy Paste

S1

```
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
%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#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
Fa0/22 disabled 999 auto auto 10/100BaseTX
--More-->
```

Top

Copy Paste

Step 4: Document and implement port security features.

The interfaces F0/6 on S1 and F0/18 on S2 are configured as access ports. In this step, you will also

configure port security on these two access ports.

1. On S1, issue the **show port-security interface f0/6** command to display the default port security settings for interface F0/6. Record your answers in the table below.

Default Port Security Configuration	
Feature	Default Setting
Port security	Disabled
Max. number of MAC addresses	1
Violation mode	Shutdown
Aging Time	0 mins
Aging Type	Absolute
Secure Static Address Aging	Disabled
Sticky MAC Address	0

2. On S1, enable port security on F0/6 with the following settings:

- Maximum number of MAC addresses: 3
- Violation type: restrict
- Aging time: 60 min
- Aging type: inactivity

S1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

S1>enable
S1#show port-security interface f0/6
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
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#interface f0/6

% Invalid input detected at '^' marker.

S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface f0/6
S1(config-if)#switchport port-security
S1(config-if)#port-security maximum 3
^
% Invalid input detected at '^' marker.

S1(config-if)#switchport port-security maximum 3
S1(config-if)#switchport port-security violation restrict
S1(config-if)#switchport port-security aging time 60
S1(config-if)#switchport port-security aging type inactivity
^
% Invalid input detected at '^' marker.
S1(config-if)#


```

Top

Copy Paste

3. Verify port security on S1 F0/6 using **show port-security interface f0/6** and **show port-security address**.

S1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
S1(config-if)#switchport port-security maximum 3
S1(config-if)#switchport port-security violation restrict
S1(config-if)#switchport port-security aging time 60
S1(config-if)#switchport port-security aging type inactivity
^
% Invalid input detected at '^' marker.

S1(config-if)#show port-security interface f0/6
^
% Invalid input detected at '^' marker.

S1(config-if)#exit
S1(config)#show port-security interface f0/6
^
% Invalid input detected at '^' marker.

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

S1#show port-security interface f0/6
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#show port-security address
   Secure Mac Address Table
-----+-----+-----+-----+
Vlan  Mac Address      Type      Ports  Remaining Age
-----+-----+-----+-----+
-----+-----+-----+-----+
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 1024
S1#
```

Top

Copy Paste

4. Enable port security for F0/18 on S2. Configure the port to add MAC addresses learned on the port automatically to the running configuration.

5. Configure the following port security settings on S2 F/18:

- Maximum number of MAC addresses: 2
- Violation type: Protect
- Aging time: 60 min

6. Verify port security on S2 F0/18.

The screenshot shows a Windows desktop with a Cisco IOS CLI window titled 'S2'. The window has tabs 'Physical', 'Config', 'CLI' (which is selected), and 'Attributes'. The main pane displays the following CLI session:

```
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up

S2>enable
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface f0/18
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)#show port-security interface f0/18
% Invalid input detected at '^' marker.

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

S2#show port-security interface f0/18
Port Security           : Disabled
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#show port-security address
  Secure Mac Address Table
  -----
  VLAN    Mac Address      Type          Ports  Remaining Age
  -----  -----
  Total Addresses in System (excluding one mac per port) : 0
  Max Addresses limit in System (excluding one mac per port) : 1024
S2#
```

The taskbar at the bottom shows various application icons, and the system tray indicates the date and time as 'ENG 23:33'.

Step 5: Implement DHCP snooping security.

1. On S2, enable DHCP snooping and configure DHCP snooping on VLAN 10.
2. Configure the trunk port on S2 as a trusted port.

3. Limit the untrusted port, F18 on S2, to five DHCP packets per second.

4. Verify DHCP Snooping on S2.

```
S2>enable
S2#conf 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)#interface f0/18
S2(config-if)#ip dhcp snooping limit rate 5
S2(config-if)#show ip dhcp snooping
% Invalid input detected at '^' marker.
S2(config-if)#exit
S2(config)#
% Invalid input detected at '^' marker.
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
S2#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface          Trusted      Rate limit (pps)
FastEthernet0/1     yes        unlimited
FastEthernet0/18    no         5
S2#
```

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

C:\Users\Student> ipconfig /release

C:\Users\Student> ipconfig /renew

```
C:\>DHCP request failed.  
C:\>ipconfig /release  
IP Address.....: 0.0.0.0  
Subnet Mask.....: 0.0.0.0  
Default Gateway.: 0.0.0.0  
DNS Server.....: 0.0.0.0  
C:\>ipconfig /renew  
IP Address.....: 192.168.10.10  
Subnet Mask.....: 255.255.255.0  
Default Gateway.: 192.168.10.1  
DNS Server.....: 0.0.0.0  
C:\>ipconfig /release  
IP Address.....: 0.0.0.0  
Subnet Mask.....: 0.0.0.0  
Default Gateway.: 0.0.0.0  
DNS Server.....: 0.0.0.0  
C:\>ipconfig /renew  
IP Address.....: 192.168.10.10  
Subnet Mask.....: 255.255.255.0  
Default Gateway.: 192.168.10.1  
DNS Server.....: 0.0.0.0  
C:\>
```

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

S2# show ip dhcp snooping binding

MacAddress IpAddress Lease(sec) Type VLAN Interface

00:50:56:90:D0:8E 192.168.10.11 86213 dhcp-snooping 10 FastEthernet0/18

Total number of bindings: 1

```

S2 Physical Config CLI Attributes
IOS Command Line Interface

S2#show ip dhcp snooping statistics
% Invalid input detected at '^' marker.

S2#no ip dhcp snooping
% Invalid input detected at '^' marker.

S2#econf t
% Invalid input detected at '^' marker.

S2#conf 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)#interface f0/18
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#
$SYS-5-CONFIG_I: Configured from console by console

S2#show ip dhcp snooping binding
MacAddress          IpAddress      Lease(sec)  Type        VLAN  Interface
-----  -----
Total number of bindings: 0

S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#no ip dhcp snooping information option
S2(config)#exit
S2#
$SYS-5-CONFIG_I: Configured from console by console

S2#show ip dhcp snooping binding
MacAddress          IpAddress      Lease(sec)  Type        VLAN  Interface
-----  -----
00:0A:41:9B:98:EB  192.168.10.10    0         dhcp-snooping  10    FastEthernet0/18
Total number of bindings: 1
S2#

```

Copy Paste

Top

Step 6: Implement PortFast and BPDU guard.

1. Configure PortFast on all the access ports that are in use on both switches.

S1(config)# interface range f0/5 - 6

S1(config-if)# spanning-tree portfast

S2(config)# interface f0/18

S2(config-if)# spanning-tree portfast

S1

```

S1>enable
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface range f0/5 - 6
% Invalid input detected at '^' marker.

S1(config)#interface range f0/5 - 6
S1(config-if-range)#spanning-tree portfast
Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/5 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/6 but will only
have effect when the interface is in a non-trunking mode.
S1(config-if-range)#

```

Copy Paste

Top

S2

```

00:0A:41:9B:98:EB 192.168.10.10 0 ----- dhcp-snooping 10 FastEthernet0/18
Total number of bindings: 1
S2#


S2>enable
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface f0/18
S2(config-if)#spanning-tree portfast
Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/18 but will only
have effect when the interface is in a non-trunking mode.

```

Copy Paste

Top

2. Enable BPDU guard on S1 and S2 VLAN 10 access ports connected to PC-A and PC-B.

S1(config)# interface f0/6

```
S1(config-if)# spanning-tree bpduguard enable
```

```
S2(config)# interface f0/18
```

```
S2(config-if)# spanning-tree bpduguard enable
```

3. Verify that BPDU guard and PortFast are enabled on the appropriate ports.

```
S1# show spanning-tree interface f0/6 detail
```

Port 8 (FastEthernet0/6) of VLAN0010 is designated forwarding

Port path cost 19, Port priority 128, Port Identifier 128.6.

<output omitted for brevity>

Number of transitions to forwarding state: 1

The port is in the portfast mode

Link type is point-to-point by default

Bpdu guard is enabled

BPDU: sent 128, received 0

S1

```

Physical Config CLI Attributes
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface range f0/5
^
% Invalid input detected at '^' marker.

S1(config)#interface range f0/5 #spanning-tree portfast
S1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

#Portfast has been configured on FastEthernet0/5 but will only
have effect when the interface is in a non-trunking mode.
S1(config-if)#exit
S1(config)#interface f0/6
S1(config-if)#spanning-tree bpduguard enable
S1(config-if)#exit
S1(config)#exit
%SYS-5-CONFIG_I: Configured from console by console

S1#show spanning-tree interface f0/6 detail

Port 6 (FastEthernet0/6) of VLAN0010 is designated forwarding
Port path cost 19, Port priority 128, Port Identifier 128.6
Designated root has priority 4106, address 00D0.FF44.5AA3
Designated bridge has priority 4106, address 00D0.FF44.5AA3
Designated port has priority 4106, designated path cost 19
Timers: message age 16, forward delay 0, hold 0
Number of transitions to forwarding state: 1
The port is in the portfast mode
Link type is point-to-point by default

S1#

```

S2

```

Physical Config CLI Attributes
Enter configuration commands, one per line. End with CNTL/Z.
S2#enable
S2#conf t
S2#Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface f0/18
S2(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

#Portfast has been configured on FastEthernet0/18 but will only
have effect when the interface is in a non-trunking mode.
S2(config-if)#exit
S2(config)#interface f0/18
S2(config-if)#spanning-tree bpduguard enable
S2(config-if)#exit
S2(config)#show spanning-tree interface f0/18 detail
^
% Invalid input detected at '^' marker.

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

S2#show spanning-tree interface f0/6 detail

S2#show spanning-tree interface f0/18 detail

Port 18 (FastEthernet0/18) of VLAN0010 is designated forwarding
Port path cost 19, Port priority 128, Port Identifier 128.18
Designated root has priority 4106, address 00D0.FF44.5AA3
Designated bridge has priority 32778, address 0001.C783.E3E7
Designated port has priority 4106, designated path cost 19
Timers: message age 16, forward delay 0, hold 0
Number of transitions to forwarding state: 1
The port is in the portfast mode
Link type is point-to-point by default

S2#

```

Step 7: Verify end-to-end connectivity.

Verify PING connectivity between all devices in the IP Addressing Table. If the pings fail, you may need to disable the firewall on the PC hosts.

PC-A

Physical Config Desktop Programming Attributes

Command Prompt

```
Ping statistics for 192.168.10.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.201

Pinging 192.168.10.201 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.201: bytes=32 time<1ms TTL=255
Reply from 192.168.10.201: bytes=32 time<1ms TTL=255
Reply from 192.168.10.201: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.201:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.202

Pinging 192.168.10.202 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.202: bytes=32 time<1ms TTL=255
Reply from 192.168.10.202: bytes=32 time<1ms TTL=255
Reply from 192.168.10.202: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.202:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Top

ENG 0043

PC-B

Physical Config Desktop Programming Attributes

Command Prompt

```
Ping statistics for 192.168.10.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.201

Pinging 192.168.10.201 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.201: bytes=32 time<1ms TTL=255
Reply from 192.168.10.201: bytes=32 time<1ms TTL=255
Reply from 192.168.10.201: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.201:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.202

Pinging 192.168.10.202 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.202: bytes=32 time<1ms TTL=255
Reply from 192.168.10.202: bytes=32 time<1ms TTL=255
Reply from 192.168.10.202: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.202:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Top

ENG 0045

Questions to Answer

-
1. In reference to Port Security on S2, why is there no timer value for the remaining age in minutes when sticky learning was configured?

This switch does not support the port security aging of sticky secure addresses.

2. In reference to Port Security on S2, if you load the running-config script on S2, why will PC-B on port 18 never get an IP address via DHCP?

Port security is set for only two MAC addresses and port 18 has two “sticky” MAC address bound to the port. Additionally, the violation is protect, which will never send a console/syslog message or increment the violation counter.

3. In reference to Port Security, what is the difference between the absolute aging type and inactivity aging type?

If the inactivity type is set, then the secure addresses on the port will be removed only if there is no data traffic from the secure source addresses for the specified time period.

If the absolute type is set, then all secure addresses on this port age out exactly after the time specified ends.

Conclusion

In this practical, DHCP Snooping was successfully implemented to enhance network security by controlling DHCP message flow and preventing rogue DHCP servers from issuing unauthorized IP addresses. The configuration process demonstrated how trusted and untrusted ports determine which interfaces can send or receive DHCP server messages. During troubleshooting, it was observed that clients failed to obtain IP addresses when DHCP Snooping was misconfigured, specifically due to the insertion of DHCP Option 82 information, which the router’s DHCP server could not process. Disabling Option 82 resolved the issue, allowing proper DHCP lease allocation and binding creation.

Additionally, it was established that DHCP Snooping should be enabled on all switches with connected end devices—S1 and S2 in this case—to ensure consistent protection across the network. Trusted ports were correctly configured on uplinks to the DHCP server and between switches, while access ports remained untrusted.

Overall, this exercise reinforced key networking concepts, including VLAN configuration, DHCP operations, and Layer 2 security mechanisms, highlighting the importance of precise configuration and verification in maintaining a secure and reliable enterprise network.