Department of Computer Science and Engineering

Islamic University of Technology (IUT)

A subsidiary organ of OIC

Laboratory Report

CSE 4512: Computer Networks Lab

Name: Md Farhan Ishmam
Student ID: 180041120
Section: CSE-1
Semester: Fifth
Academic Year: 2021

Date of Submission: 10-Oct-2021

Title: Configuring Switch Port Security in Cisco Devices

Objective:

1. Describe the concept of Switch Port Security
2. Explain the importance of Switch Port Security in securing an organization
3. Configure Switch Port Security in CISCO devices
4. Use the Switch Port Security feature to achieve varying degrees of protection

Devices/ Software Used:

1. Device: Windows PC
2. Software: Cisco Packet Tracer 7.3.0

Theory:

Ways of Learning and limiting MAC addresses on a secure port:
To set the maximum number of MAC addresses allowed on a port, we use the following command:

```
Switch(config-if)# switchport port-security maximum value
```

The default number allowed MAC address is 1. The maximum number of allowed MAC addresses that can be configured depending on the switch and the IOS. In this example, the maximum is 8192.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security maximum ?
 <1-8192> Maximum addresses
```

The switch has three ways to learn about the MAC addresses on a secure port:

1. **Manually Configured**

The administrator manually configures the allowed static MAC address by using the following command:

```
Switch(config-if)# switchport port-security mac-address mac-address
```

If the device MAC addresses are known and do not change often then the administrator can specify those beforehand. If you want no other device to be connected to the given port than those you'd specify manually, you'd have to set the maximum value accordingly using the command mentioned earlier.

2. **Dynamically Learned**

This is the default learning method when you enable switchport security. After enabling, the MAC address of any device connected to the port is automatically added to the allowed list. The MAC addresses learned dynamically are not added to the startup configuration automatically. If the switch is rebooted, the port will have to re-learn the device's MAC address. This option is usually used if the host(s) connected to the port is always changing and you want to limit the number of connected hosts to a port in a given time.

3. **Dynamically Learned – Sticky**

The administrator can enable the switch to dynamically learn the MAC address and "stick" them to the running configuration by using the following command:

```
 Switch(config-if)# switchport port-security mac-address sticky
```

Saving the running configuration will commit the dynamically learned MAC address to NVRAM.

Port security aging:

This option specifies the expiry time of the learned MAC addresses. The command to enable aging is switchport port-security aging time time_in_minutes. By default, aging is not enabled and addresses are not deleted unless the device is rebooted or the MAC addresses are cleared.

Two types of aging are supported per port:

- Absolute - The allowed addresses on the port are deleted after the specified aging time.
- Inactivity - The allowed addresses on the port are deleted only if they are inactive for the specified aging time. Here, inactive means no data traffic from the specified MAC address.

The aging feature is useful if you want to grant access to certain devices only for a specified period. There's no aging for sticky MAC addresses. By default, manually allowed MAC addresses also don't have aging. But you can specify aging for those by using the static option. So, the overall format of the command with all the available options is:

```
Switch(config-if)# switchport port-security aging { static | time
time_in_minutes | type {absolute | inactivity}}
```

Note that, if the time_in_minutes is 0 it means no aging.

Port security violations

Finally, the last option is the violations option. These options basically will tell what to do if any security violations occur. A switchport violation occurs in one of two situations:

- When the maximum number of allowed MAC addresses is crossed
- An address learned or configured on one secure port is seen on another secure port in the same VLAN

The action to be taken after a violation is set using any of the following modes:

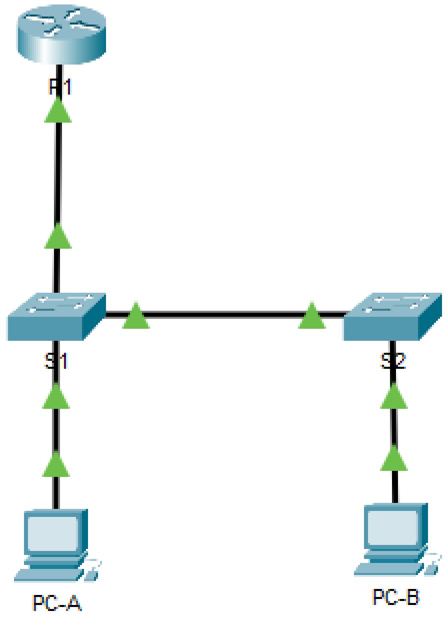
- **Protect** — This mode permits traffic from known MAC addresses to continue to be forwarded while dropping traffic from unknown MAC addresses when over the allowed MAC address limit. When configured with this mode, no notification action is taken when traffic is dropped.

- **Restrict** — This mode permits traffic from known MAC addresses to continue to be forwarded while dropping traffic from unknown MAC addresses when over the allowed MAC address limit. When configured with this mode, a Syslog message is logged and a violation counter is incremented when traffic is dropped.

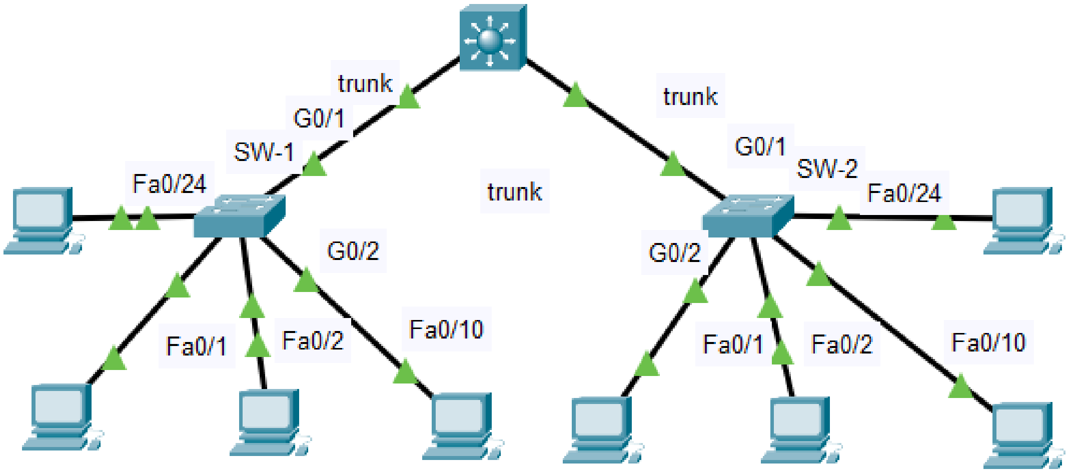
- **Shutdown** — This mode is the default violation mode; when in this mode, the switch will automatically force the switchport into an error-disabled (err-disable) state when a violation occurs. While in this state, the switchport forwards no traffic. The switchport can be brought out of this error disabled state by issuing the by disabling and re-enabling the switchport.

Diagram of the experiment:

Task-1:



Task-2:

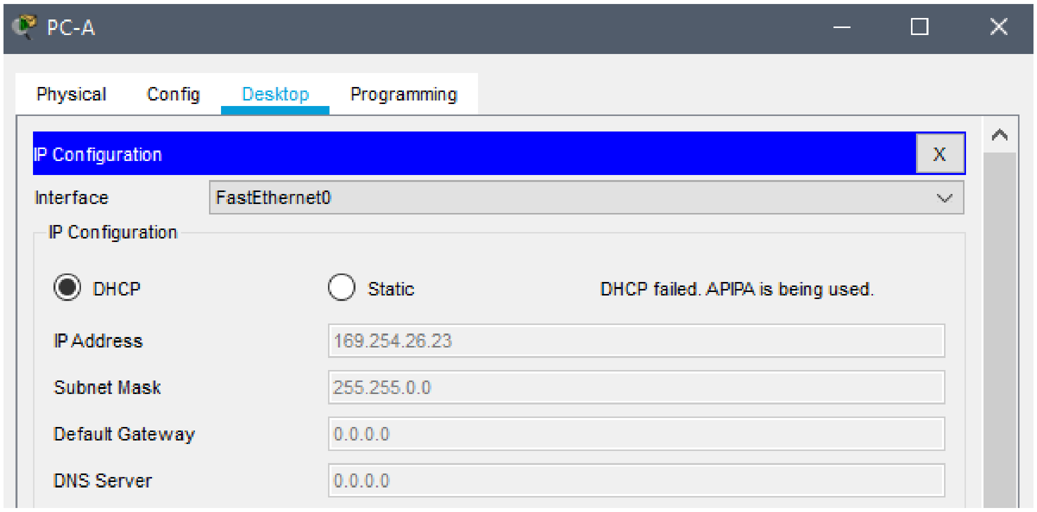


Working Procedure:

Part 1: Configure the Network Devices

Step 1: Cable the network

a. We cable the network as shown in the topology by taking a router, two switches, and two PCs
b. The devices are initialized along with some basic configurations like enabling DHCP in the PCs to dynamically allocate the IP address as instructed in the Addressing Table.



IP Configuration

Interface FastEthernet0

IP Configuration

● DHCP ○ Static DHCP failed. APIPA is being used.

IP Address 169.254.26.23

Subnet Mask 255.255.0.0

Default Gateway 0.0.0.0

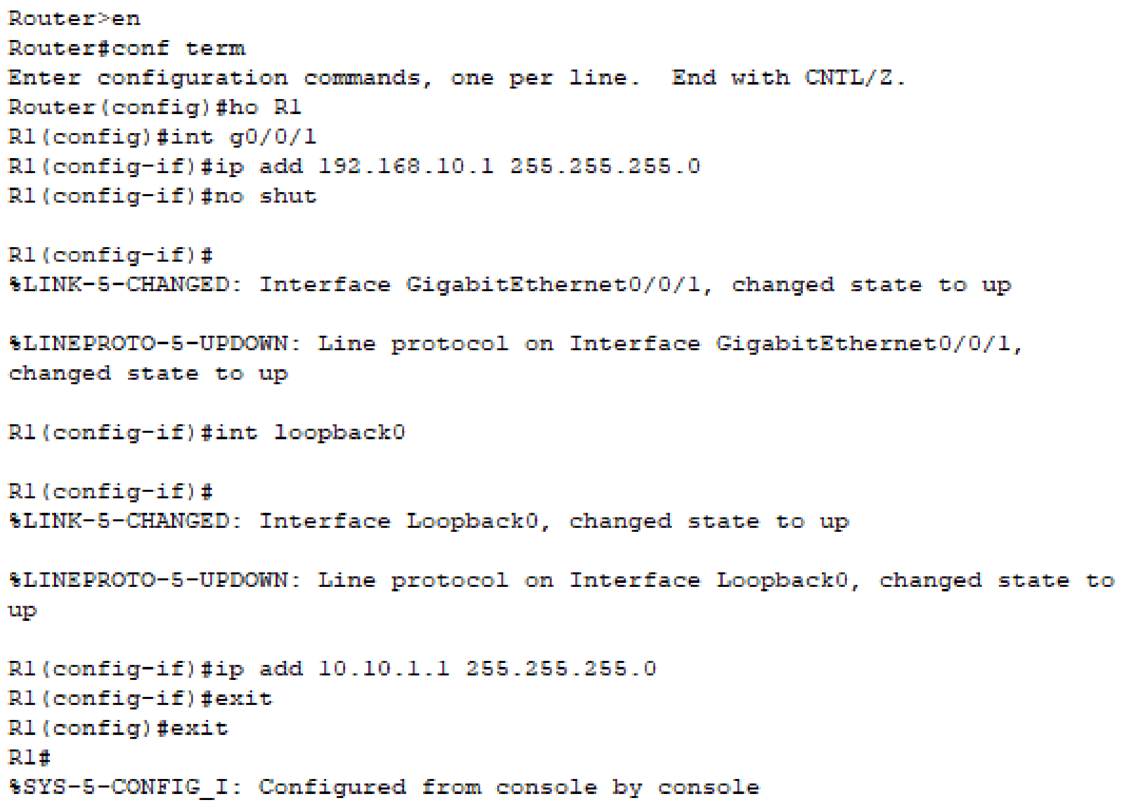
DNS Server 0.0.0.0

Step 2: Configure R1 (follow network configuration table)

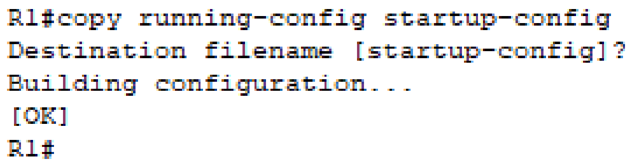
The router R1 was configured by going to the configuration mode, changing the hostname, and then configuring the interfaces according to the configuration table. Afterward, the configuration was saved to the startup-config file. The following commands were used to configure the router R1. R2 was configured similarly.

```
Router>en
Router#conf term
Router(config)#ho R1
R1(config)#int g0/0/1
R1(config-if)#ip add 192.168.10.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int loopback0
R1(config-if)#ip add 10.10.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#exit
R1#copy running-config startup-config
```

R1:



```
Router>en
Router#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ho R1
R1(config)#int g0/0/1
R1(config-if)#ip add 192.168.10.1 255.255.255.0
R1(config-if)#no shut

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)#int loopback0

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to
up

R1(config-if)#ip add 10.10.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```



```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

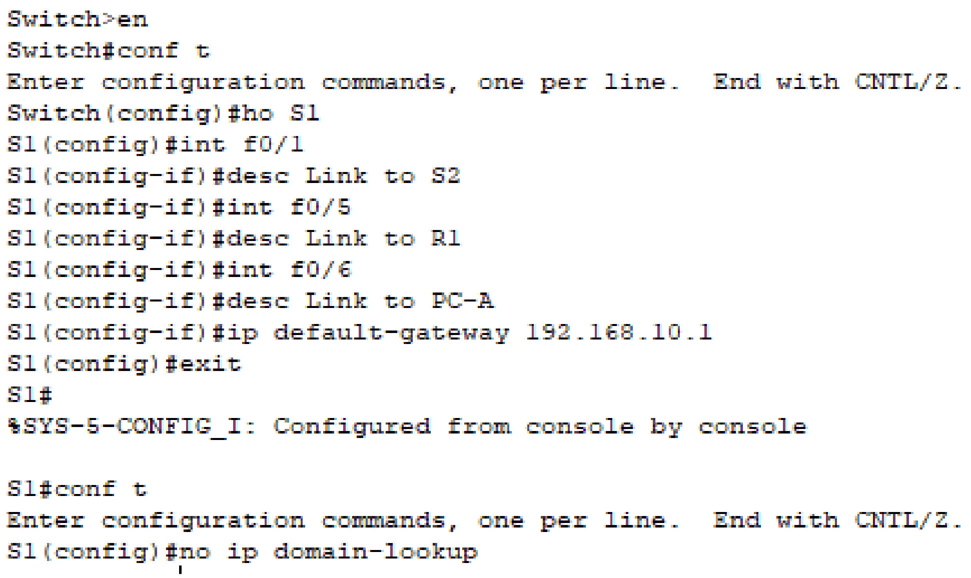
Step 3: Configure and verify basic switch settings.

a. Configure the hostname for switches S1 and S2
b. Prevent unwanted DNS lookups on both switches.
c. Configure interface descriptions for the ports that are in use in S1 and S2.
d. Set the default gateway for the Management VLAN to 192.168.10.1 on both switches.

The following commands were used to configure S1:

```
Switch>en
Switch#conf t
Switch(config)#ho S1
S1(config)#no ip domain-lookup
S1(config)#int f0/1
S1(config-if)#desc Link to S2
S1(config-if)#int f0/5
S1(config-if)#desc Link to R1
S1(config-if)#int f0/6
S1(config-if)#desc Link to PC-A
S1(config-if)#ip default-gateway 192.168.10.1
S1(config)#exit
```

S1:

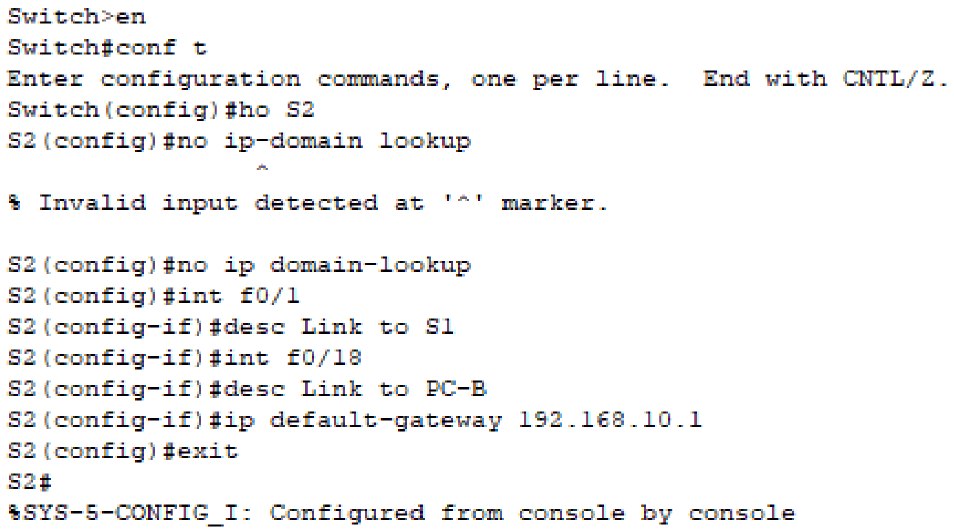


```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ho S1
S1(config)#int f0/1
S1(config-if)#desc Link to S2
S1(config-if)#int f0/5
S1(config-if)#desc Link to R1
S1(config-if)#int f0/6
S1(config-if)#desc Link to PC-A
S1(config-if)#ip default-gateway 192.168.10.1
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#no ip domain-lookup
```

The following commands were used to configure S2:

```
Switch>en
Switch#conf t
Switch(config)#ho S2
S2(config)#no ip domain-lookup
S2(config)#int f0/1
S2(config-if)#desc Link to S1
S2(config-if)#int f0/18
S2(config-if)#desc Link to PC-B
S2(config-if)#ip default-gateway 192.168.10.1
S2(config)#exit
```

S2:



```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ho S2
S2(config)#no ip-domain lookup
                ^
% Invalid input detected at '^' marker.

S2(config)#no ip domain-lookup
S2(config)#int f0/1
S2(config-if)#desc Link to S1
S2(config-if)#int f0/18
S2(config-if)#desc Link to PC-B
S2(config-if)#ip default-gateway 192.168.10.1
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
```

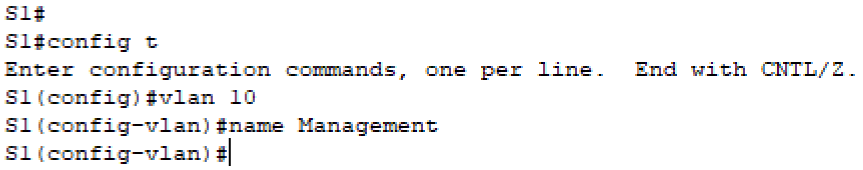
Part 2: Configure VLANs on Switches

Step 1: Configure VLAN 10

Add VLAN 10 to S1 and S2 and name the VLAN Management. The following commands were used to configure the S1:

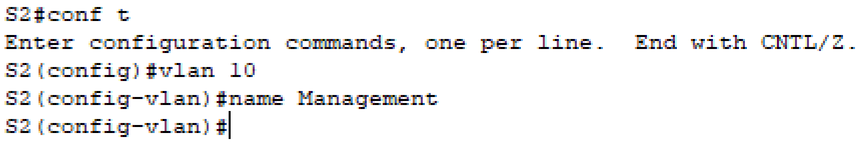
```
S1(config)#vlan 10
S1(config-vlan)#name Management
```

S1:



```
S1#
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#
```

S2:



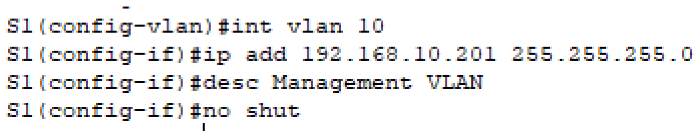
```
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#vlan 10
S2(config-vlan)#name Management
S2(config-vlan)#
```

Step 2: Configure the SVI for VLAN 10

Configure the IP address according to the Addressing Table for SVI for VLAN 10 on S1 and S2. Enable the SVI interfaces and describe the interface. The following commands were used to configure the S1:

```
S1(config-vlan)#int vlan 10
S1(config-if)#ip add 192.168.10.201 255.255.255.0
S1(config-if)#desc Management VLAN
S1(config-if)#no shut
```

S1:



```
S1(config-vlan)#int vlan 10
S1(config-if)#ip add 192.168.10.201 255.255.255.0
S1(config-if)#desc Management VLAN
S1(config-if)#no shut
```

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

The following commands were used to configure the S1:

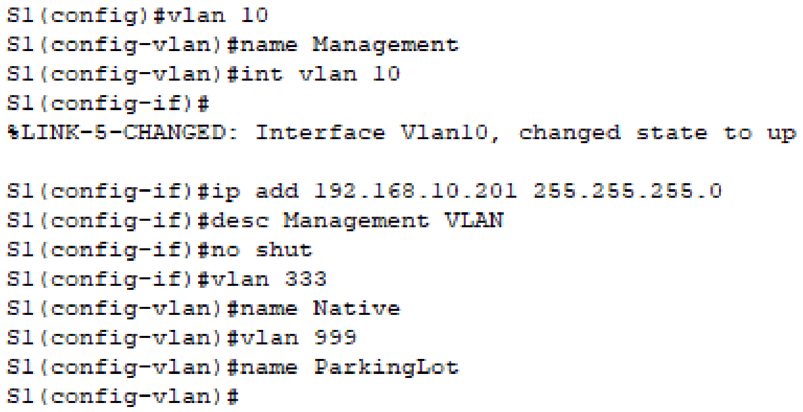
```
S1(config-if)#vlan 333
S1(config-vlan)#name Native
```

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

The following commands were used to configure the S1:

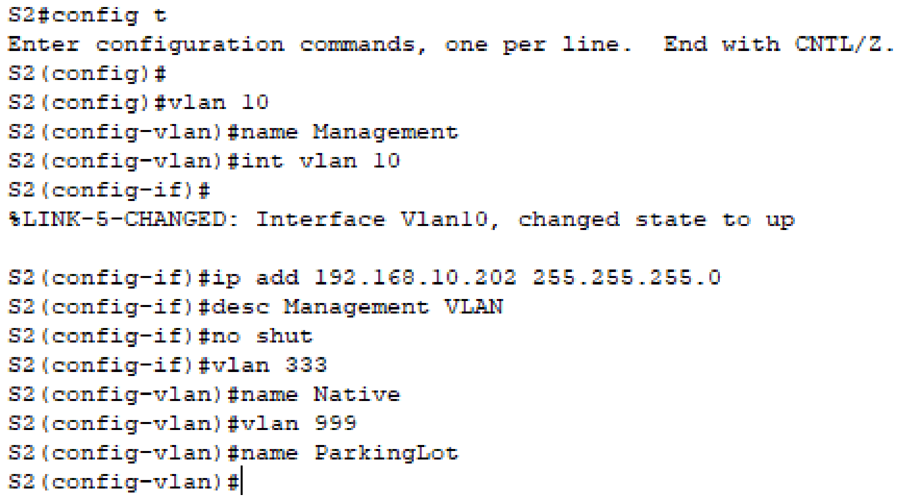
```
S1(config-vlan)#vlan 999
S1(config-vlan)#name ParkingLot
```

S1:



```
S1(config)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#int vlan 10
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

S1(config-if)#ip add 192.168.10.201 255.255.255.0
S1(config-if)#desc Management VLAN
S1(config-if)#no shut
S1(config-if)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#vlan 999
S1(config-vlan)#name ParkingLot
S1(config-vlan)#
```

S2:



```
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#
S2(config)#vlan 10
S2(config-vlan)#name Management
S2(config-vlan)#int vlan 10
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

S2(config-if)#ip add 192.168.10.202 255.255.255.0
S2(config-if)#desc Management VLAN
S2(config-if)#no shut
S2(config-if)#vlan 333
S2(config-vlan)#name Native
S2(config-vlan)#vlan 999
S2(config-vlan)#name ParkingLot
S2(config-vlan)#
```

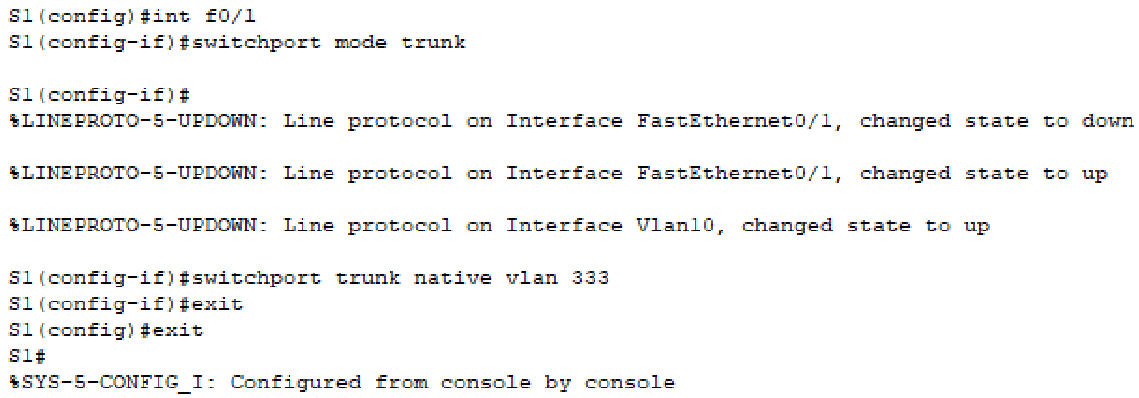
Part-3

Step 1: Implement 802.1Q trunking.

a. On both switches, configure trunking on F0/1 to use VLAN 333 as the native VLAN.
The commands for S1:

```
S1(config-vlan)#int f0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 333
```

S1:

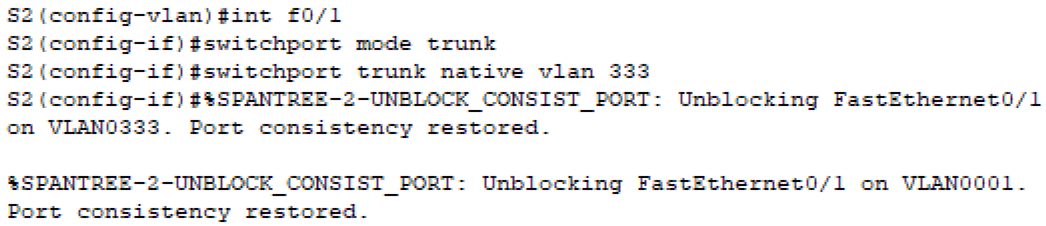


```
S1(config)#int f0/1
S1(config-if)#switchport mode trunk

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

The commands for S2:

```
S2(config-vlan)#int f0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 333
```

S2:



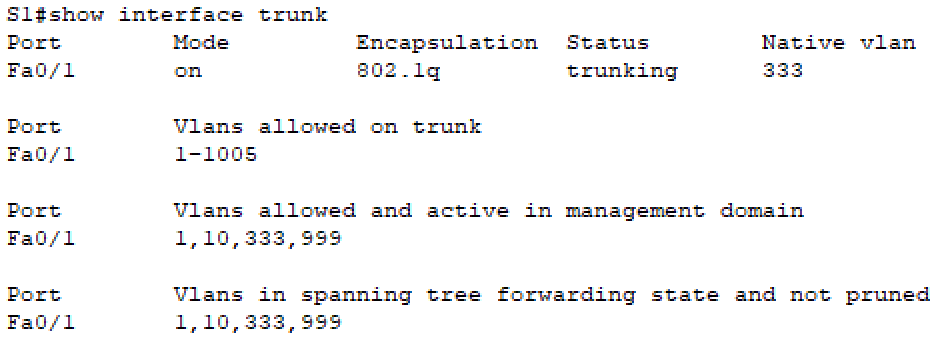
```
S2(config-vlan)#int f0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 333
S2(config-if)#%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1
on VLAN0333. Port consistency restored.

%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0001.
Port consistency restored.
```

b. Verify that trunking is configured on both switches.

The following command is used on both of the switches:

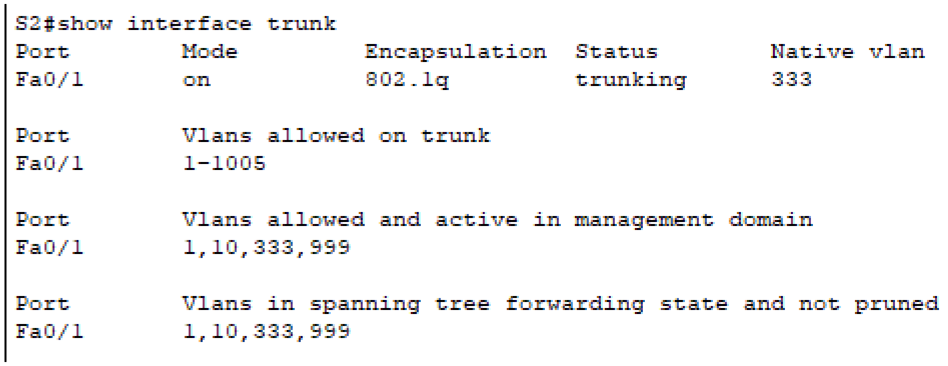
```
S1# show interface trunk
```

S1:



```
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
```

S2:



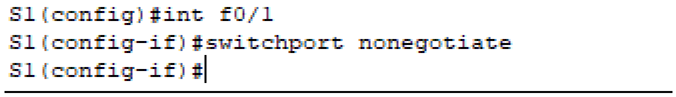
```
S2#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      333

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
```

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

The following commands were used for S1:

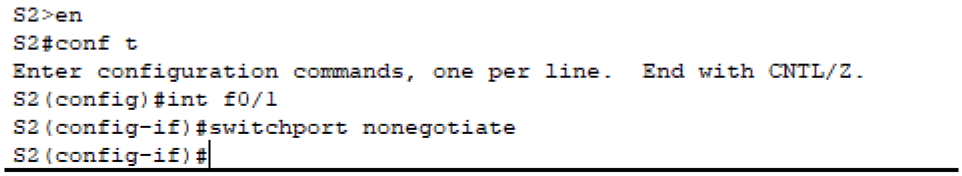
```
S1(config)#int f0/1
S1(config-if)#switchport nonegotiate
```

S1:



```
S1(config)#int f0/1
S1(config-if)#switchport nonegotiate
S1(config-if)#
```

S2:



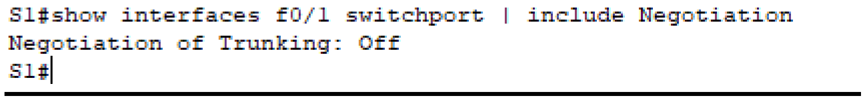
```
S2>en
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int f0/1
S2(config-if)#switchport nonegotiate
S2(config-if)#
```

d. Verify with the show interfaces command.

The following commands were used for S1:

```
S1# show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
```

S1:

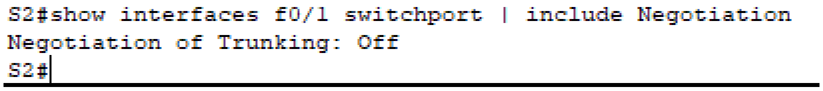


```
S1#show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
S1#
```

The commands for S2 are:

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

S2:



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

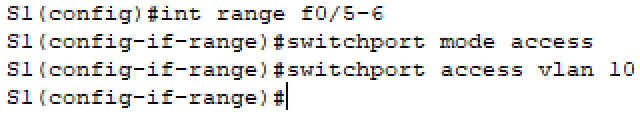
Step 2: Configure access ports.

a. On S1, configure F0/5 and F0/6 as access ports that are associated with VLAN 10.

The following commands were used for S1:

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

S1:

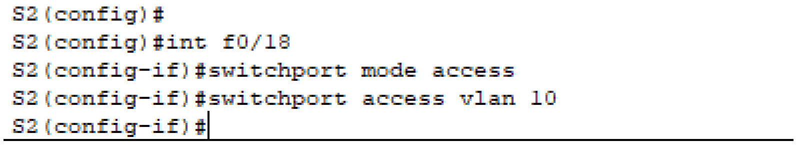


```
S1(config)#int range f0/5-6
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 10
S1(config-if-range)#
```

b. On S2, configure F0/18 as an access port that is associated with VLAN 10.
The following commands were used for S2:

```
S2(config)#int f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
```

S2:



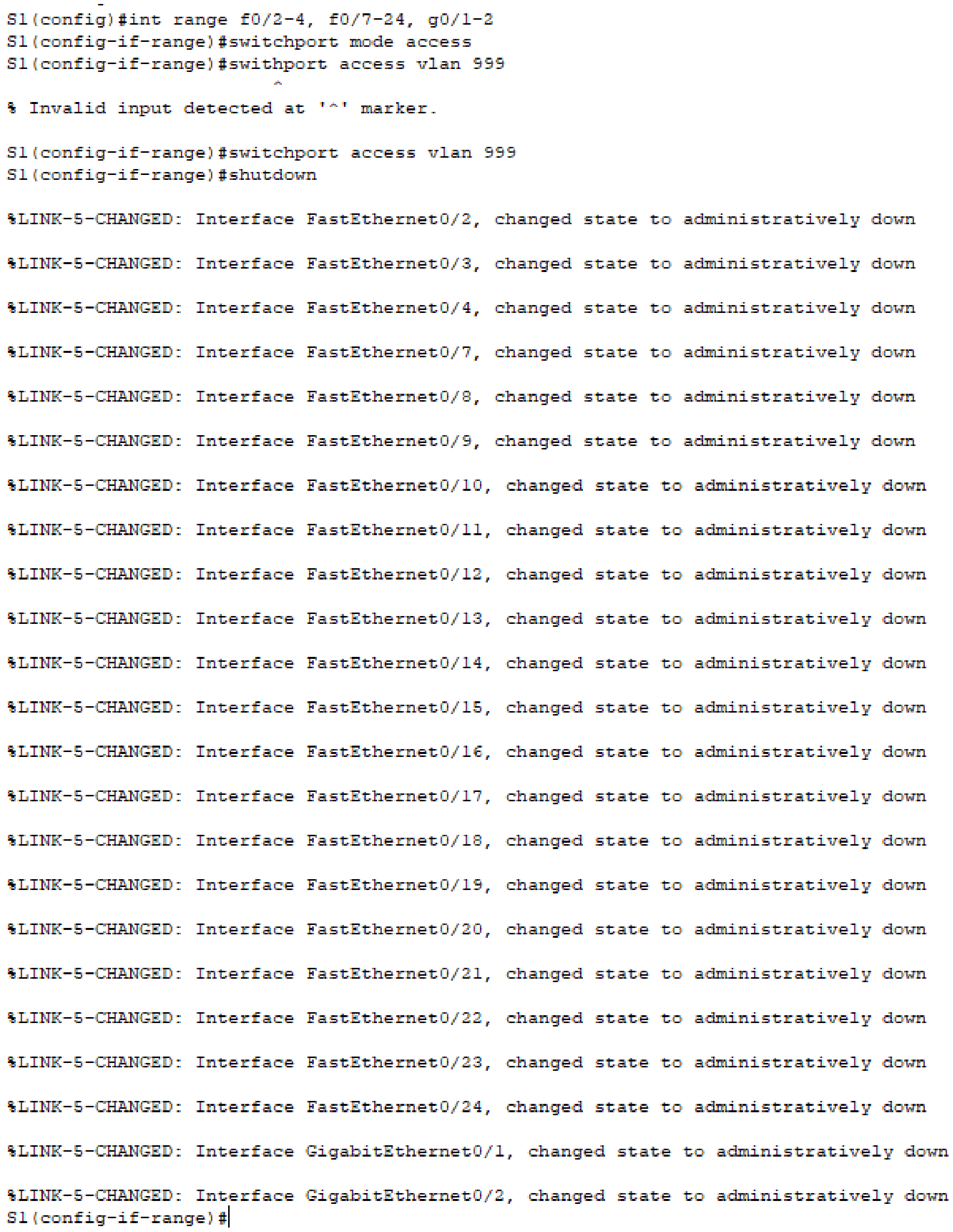
```
S2(config)#
S2(config)#int f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#
```

Step 3: Secure and disable unused switch ports.

a. On S1 and S2, move the unused ports from VLAN 1 to VLAN 999 and disable the unused ports. The following commands were used for S1:

```
S1(config)#int range f0/2-4, f0/7-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#swithport access vlan 999
```

S1:

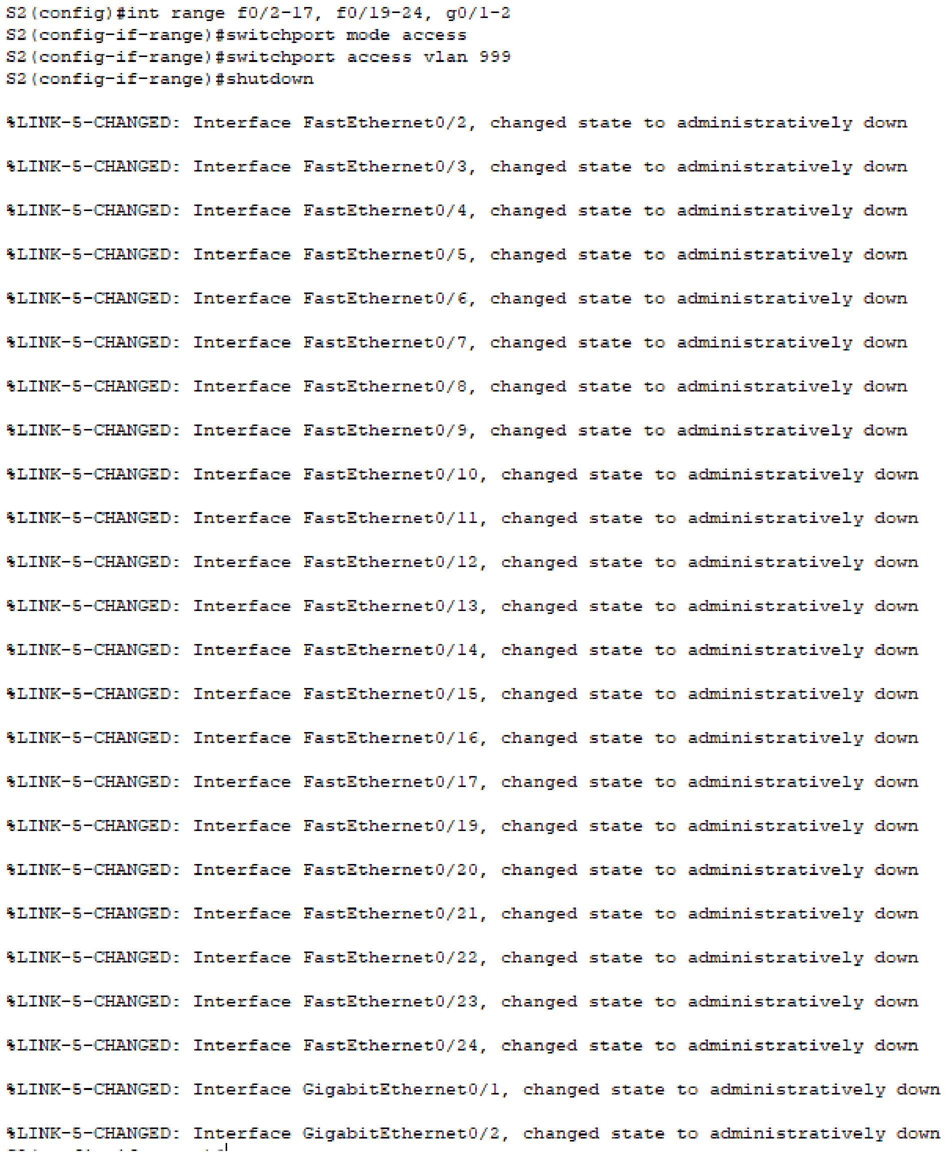


```
S1(config)#int range f0/2-4, f0/7-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#swithport access vlan 999
                        ^
% Invalid input detected at '^' marker.

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

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%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)#
```

The following commands were used for S2:

```
S2(config)#int 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
```

S2:



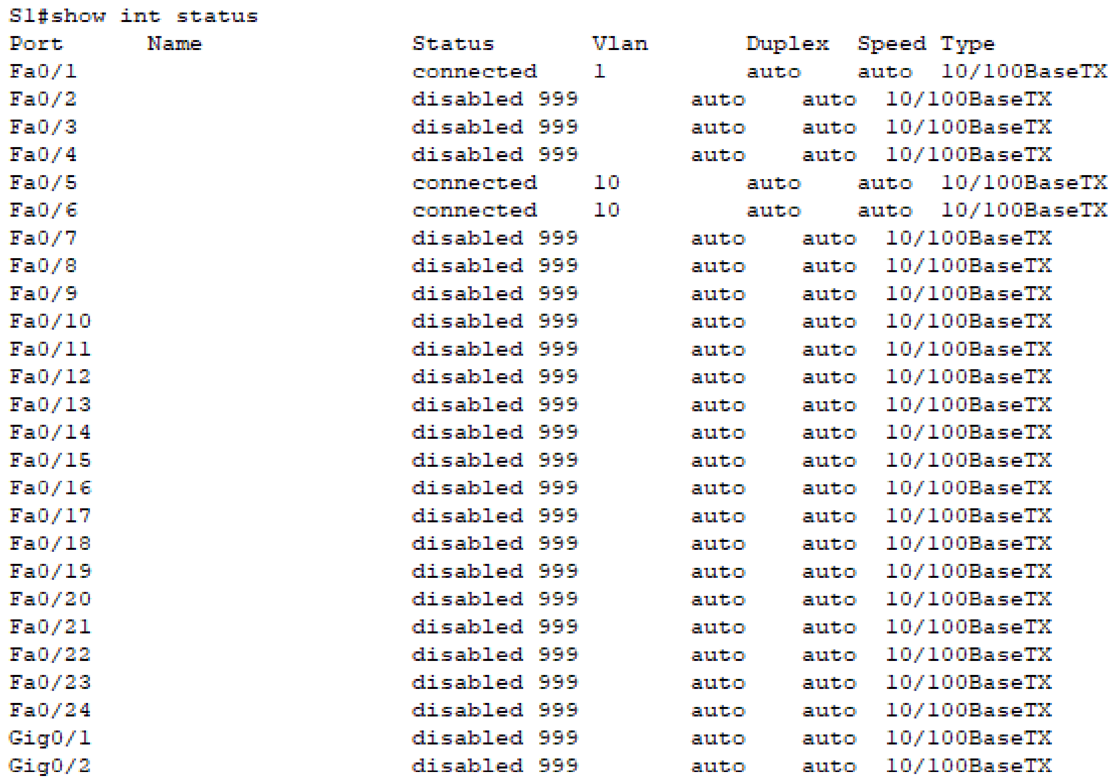
```
S2(config)#int range f0/2-17, f0/19-24, g0/1-2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 999
S2(config-if-range)#shutdown

%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

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%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
```

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

The following command was used:

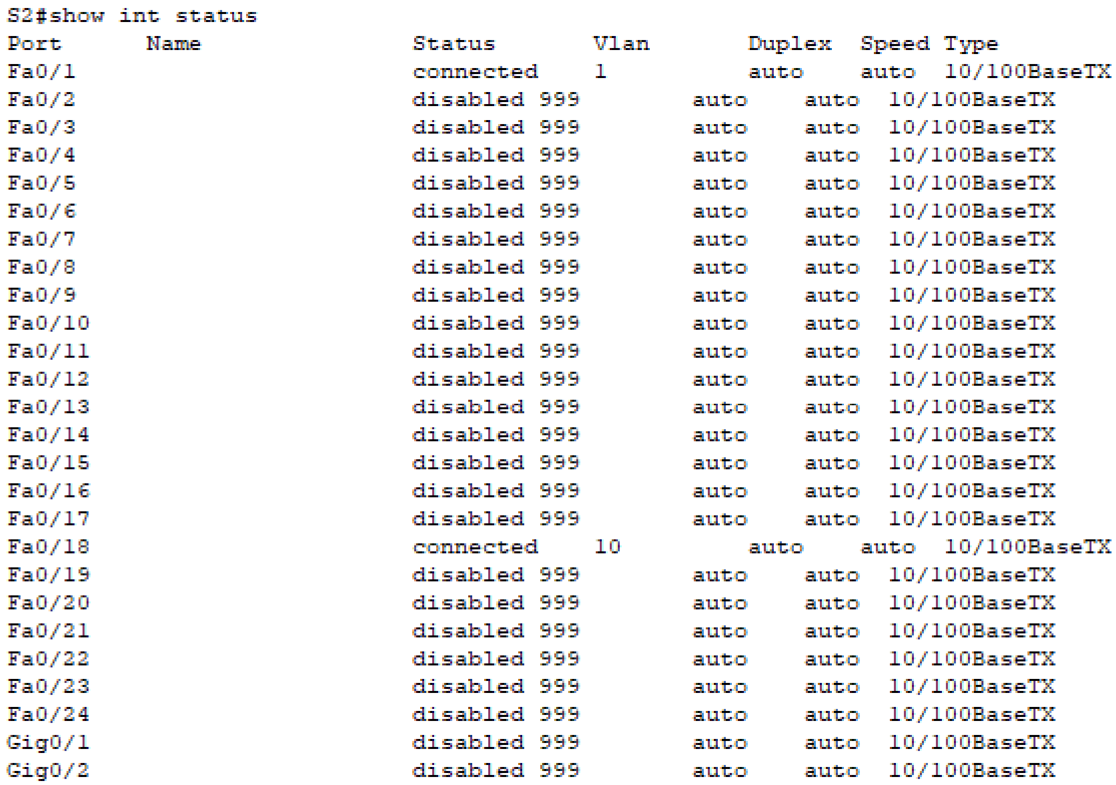
```
S1# show interfaces status
```

S1:



```
S1#show int status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    1          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                        connected    10         auto    auto  10/100BaseTX
Fa0/6                        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
Fa0/23                       disabled 999        auto    auto  10/100BaseTX
Fa0/24                       disabled 999        auto    auto  10/100BaseTX
Gig0/1                       disabled 999        auto    auto  10/100BaseTX
Gig0/2                       disabled 999        auto    auto  10/100BaseTX
```

S2:

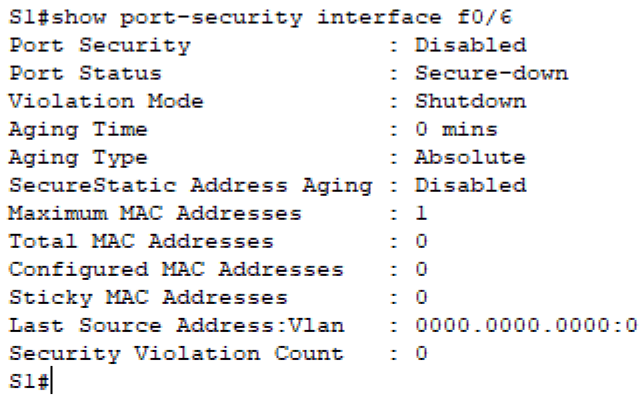


```
S2#show int status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    1          auto    auto  10/100BaseTX
Fa0/2                        disabled 999        auto    auto  10/100BaseTX
Fa0/3                        disabled 999        auto    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                       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
Fa0/22                       disabled 999        auto    auto  10/100BaseTX
Fa0/23                       disabled 999        auto    auto  10/100BaseTX
Fa0/24                       disabled 999        auto    auto  10/100BaseTX
Gig0/1                       disabled 999        auto    auto  10/100BaseTX
Gig0/2                       disabled 999        auto    auto  10/100BaseTX
```

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, we will also configure port security on these two access ports.

a. 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.



```
S1#show port-security interface f0/6
Port Security              : Disabled
Port Status                : Secure-down
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#
```

Default Port Security Configuration	
Feature	**Default Setting**
Port Security	Disabled
Maximum number of MAC addresses	1
Violation Mode	Shutdown
Aging Time	0
Aging Type	Absolute
Secure Static Address Aging	Disabled
Sticky MAC Address	0

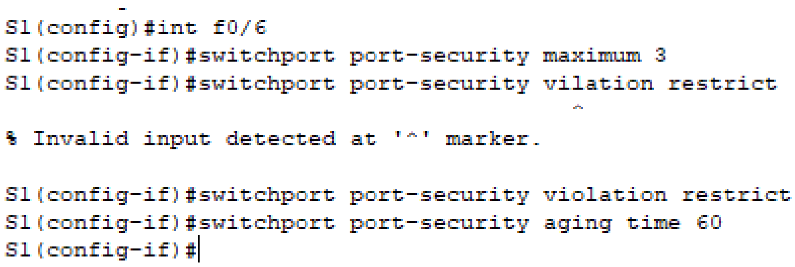
b. On S1, enable port security on F0/6 with the following settings:

o Max number of MAC addresses: 3
o Violation type: restrict
o Aging time: 60 min
o Aging type: inactivity

The following commands were used for S1:

```
S1(config) # int f0/6
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:

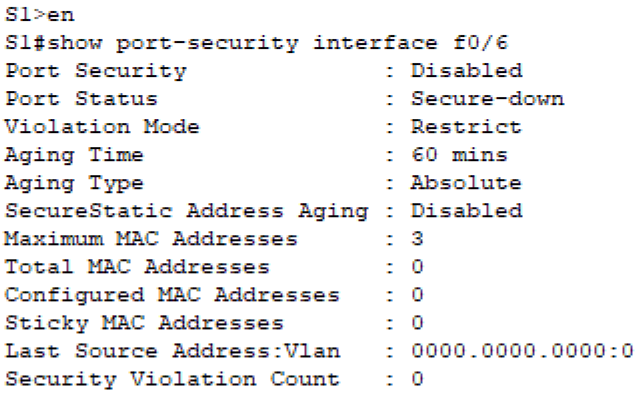


```
S1(config)#int f0/6
S1(config-if)#switchport port-security maximum 3
S1(config-if)#switchport port-security vilation restrict
                                         ^
% Invalid input detected at '^' marker.

S1(config-if)#switchport port-security violation restrict
S1(config-if)#switchport port-security aging time 60
S1(config-if)#
```

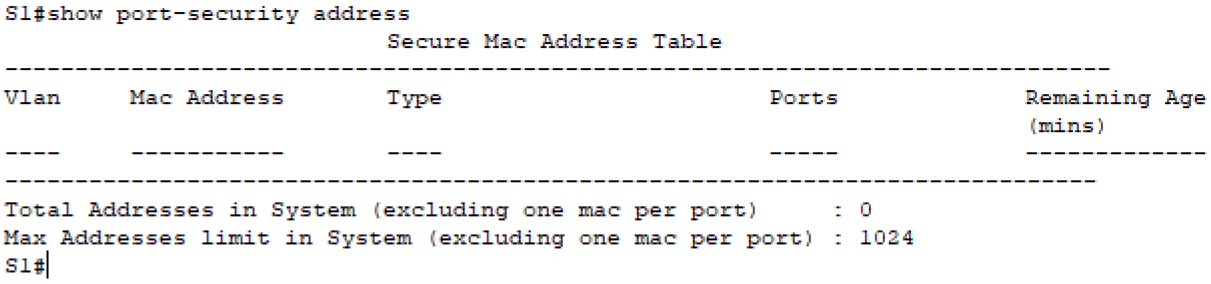
c. Verify port security on S1 F0/6. The following command was used:

```
S1# show port-security interface f0/6
S1# show port-security address
```

S1:



```
S1>en
S1#show port-security interface f0/6
Port Security              : Disabled
Port Status                : Secure-down
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
```

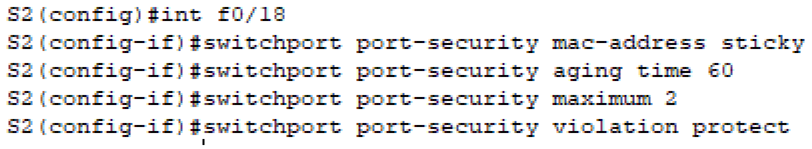


```
S1#show port-security address
                           Secure Mac Address Table
------------------------------------------------------------------------------
Vlan     Mac Address       Type                       Ports             Remaining Age
                                                 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

d. Enable port security for F0/18 on S2. Configure the port to add MAC addresses learned on the port automatically to the running configuration. The following commands were used:

```
S2(config) # int f0/18
S2(config-if)# switchport port-security mac-address sticky
S2(config-if)# switchport port-security maximum 2
S2(config-if)# switchport port-security violation protect
S2(config-if)# switchport port-security aging time 60
```

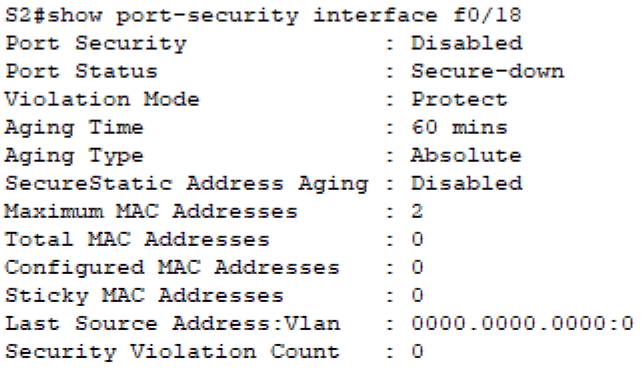
S2:



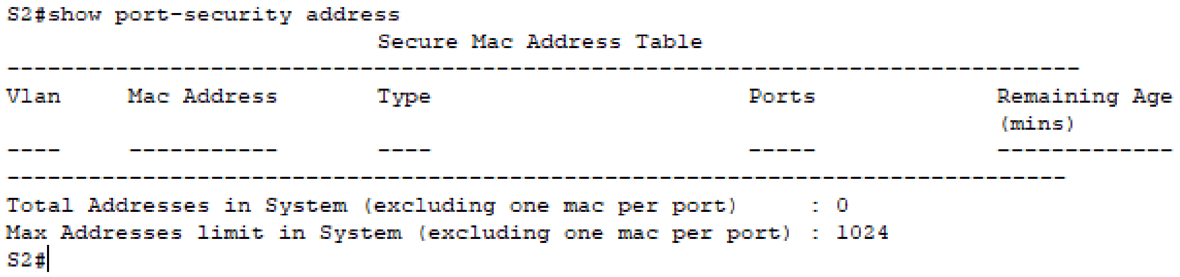
```
S2(config)#int f0/18
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#switchport port-security aging time 60
S2(config-if)#switchport port-security maximum 2
S2(config-if)#switchport port-security violation protect
```

e. Verify port security on S2 F0/18. The same commands are used for S2 which we used for S1.

S2:



```
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
```

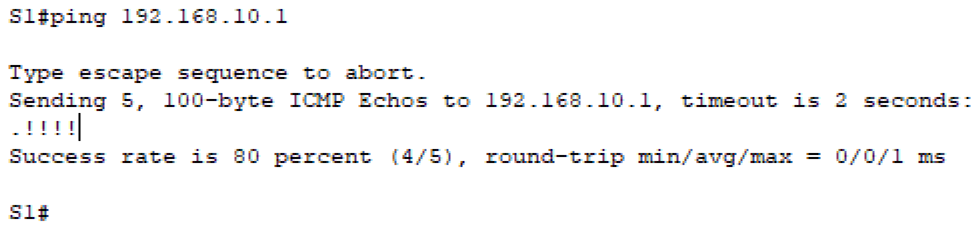


```
S2#show port-security address
                           Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan     Mac Address       Type                       Ports            Remaining Age
                                                                       (mins)
----     -----------       ----                       -----            -------------
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
S2#
```

Step 5: Verify end-to-end connectivity

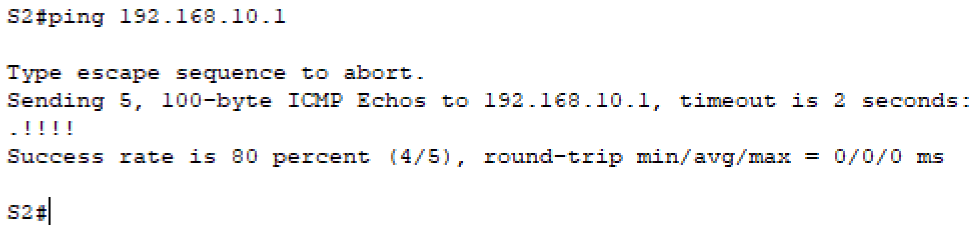
Verify PING connectivity between all devices in the IP Addressing Table. If the pings fail, you may need to disable the firewall on the PC hosts.

Pinging R1 from S1:



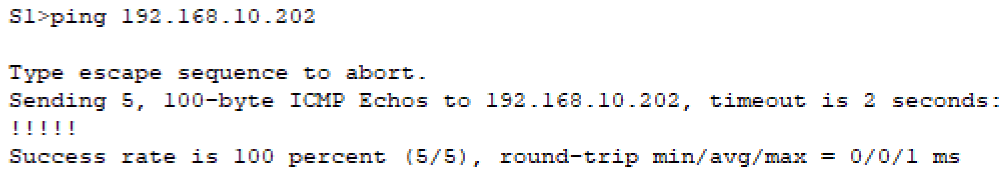
```
S1#ping 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

S1#
```

Pinging R1 from S2:



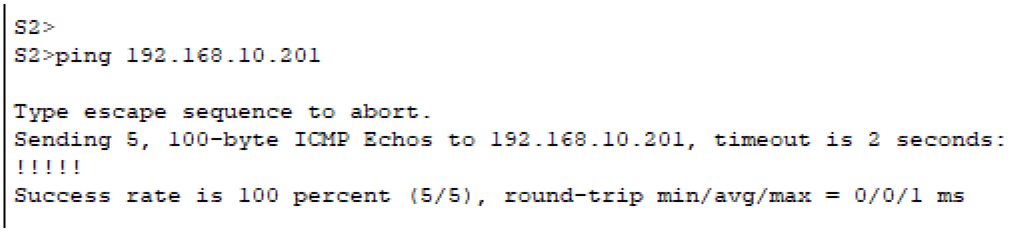
```
S2#ping 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

S2#
```

Pinging S2 from S1:



```
S1>ping 192.168.10.202

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.202, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Pinging S1 from S2:



```
S2>
S2>ping 192.168.10.201

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.201, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Task-2

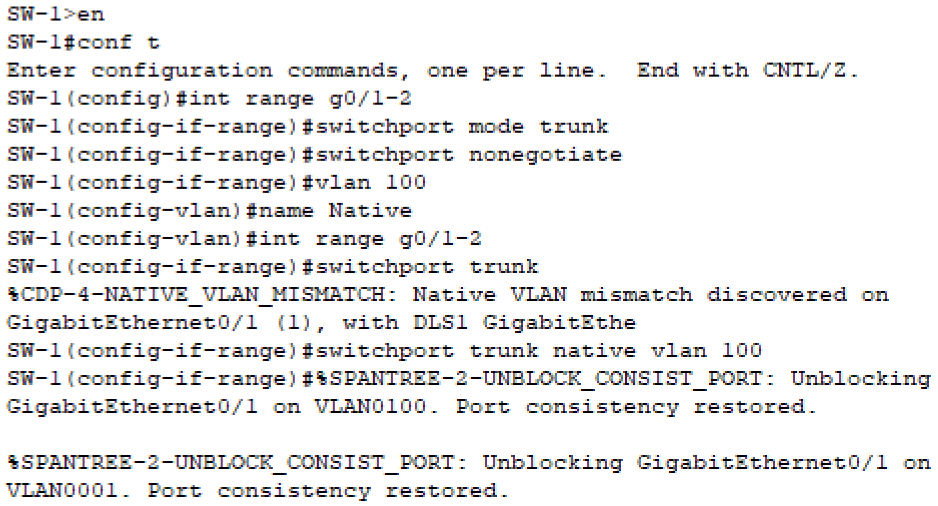
Step 1: Create a Secure Trunk

a. Connect the G0/2 ports of the two access layer switches.
b. Configure ports G0/1 and G0/2 as static trunks on both switches.
c. Disable DTP negotiation on both sides of the link.
d. Create VLAN 100 and give it the name Native on both switches.
e. Configure all trunk ports on both switches to use VLAN 100 as the native VLAN.

The following commands were used for SW-1:

```
SW-1(config)#int range g0/1-2
SW-1(config-if-range)#switchport mode trunk
SW-1(config-if-range)#switchport nonegotiate
SW-1(config-if-range)#vlan 100
SW-1(config-vlan)#name Native
SW-1(config-vlan)#int range g0/1-2
SW-1(config-if-range)#switchport trunk
SW-1(config-if-range)#switchport trunk native vlan 100
```

S1:

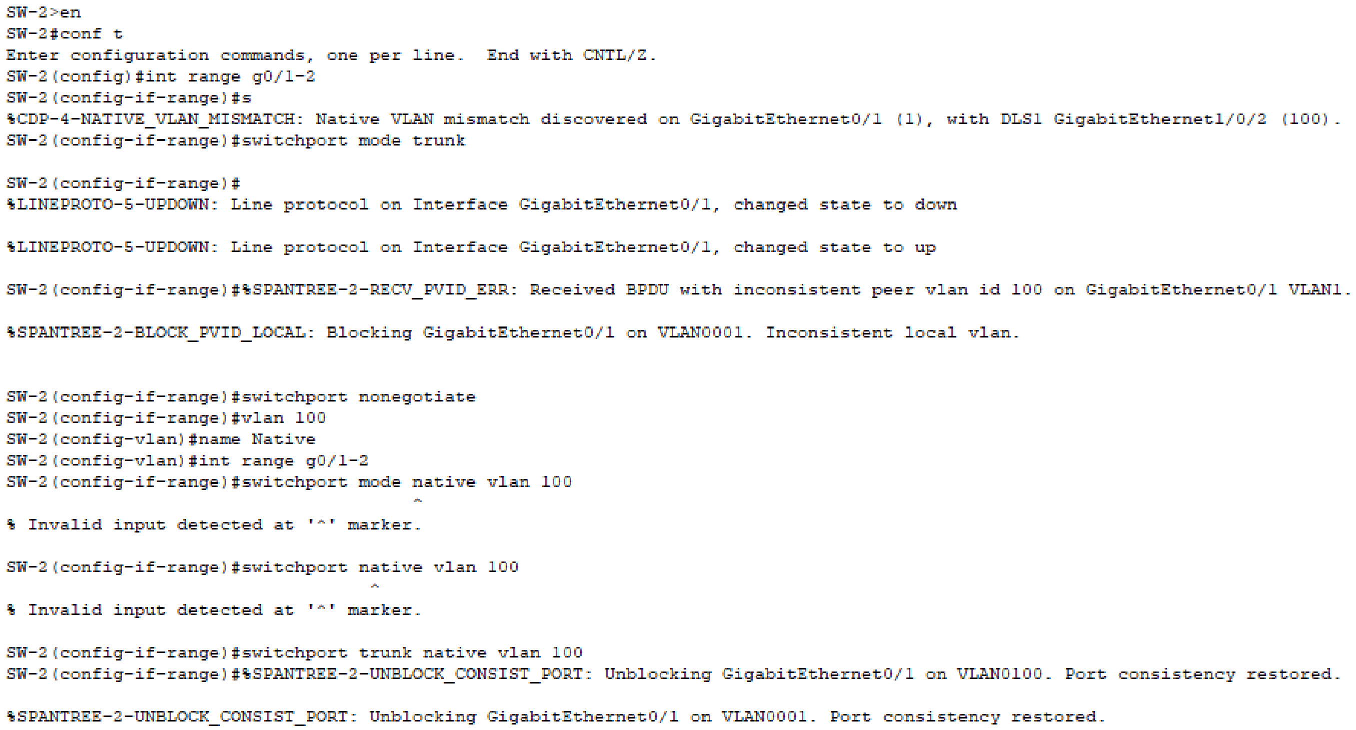


```
SW-1>en
SW-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-1(config)#int range g0/1-2
SW-1(config-if-range)#switchport mode trunk
SW-1(config-if-range)#switchport nonegotiate
SW-1(config-if-range)#vlan 100
SW-1(config-vlan)#name Native
SW-1(config-vlan)#int range g0/1-2
SW-1(config-if-range)#switchport trunk
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
GigabitEthernet0/1 (1), with DLS1 GigabitEthe
SW-1(config-if-range)#switchport trunk native vlan 100
SW-1(config-if-range)#%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking
GigabitEthernet0/1 on VLAN0100. Port consistency restored.

%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking GigabitEthernet0/1 on
VLAN0001. Port consistency restored.
```

The following commands were used for SW-2:

```
SW-2(config)#int range g0/1-2
SW-2(config-if-range)#switchport mode trunk
SW-2(config-if-range)#switchport nonegotiate
SW-2(config-if-range)#vlan 100
SW-2(config-vlan)#name Native
SW-2(config-vlan)#int range g0/1-2
SW-2(config-if-range)#switchport trunk native vlan 100
```

S2:



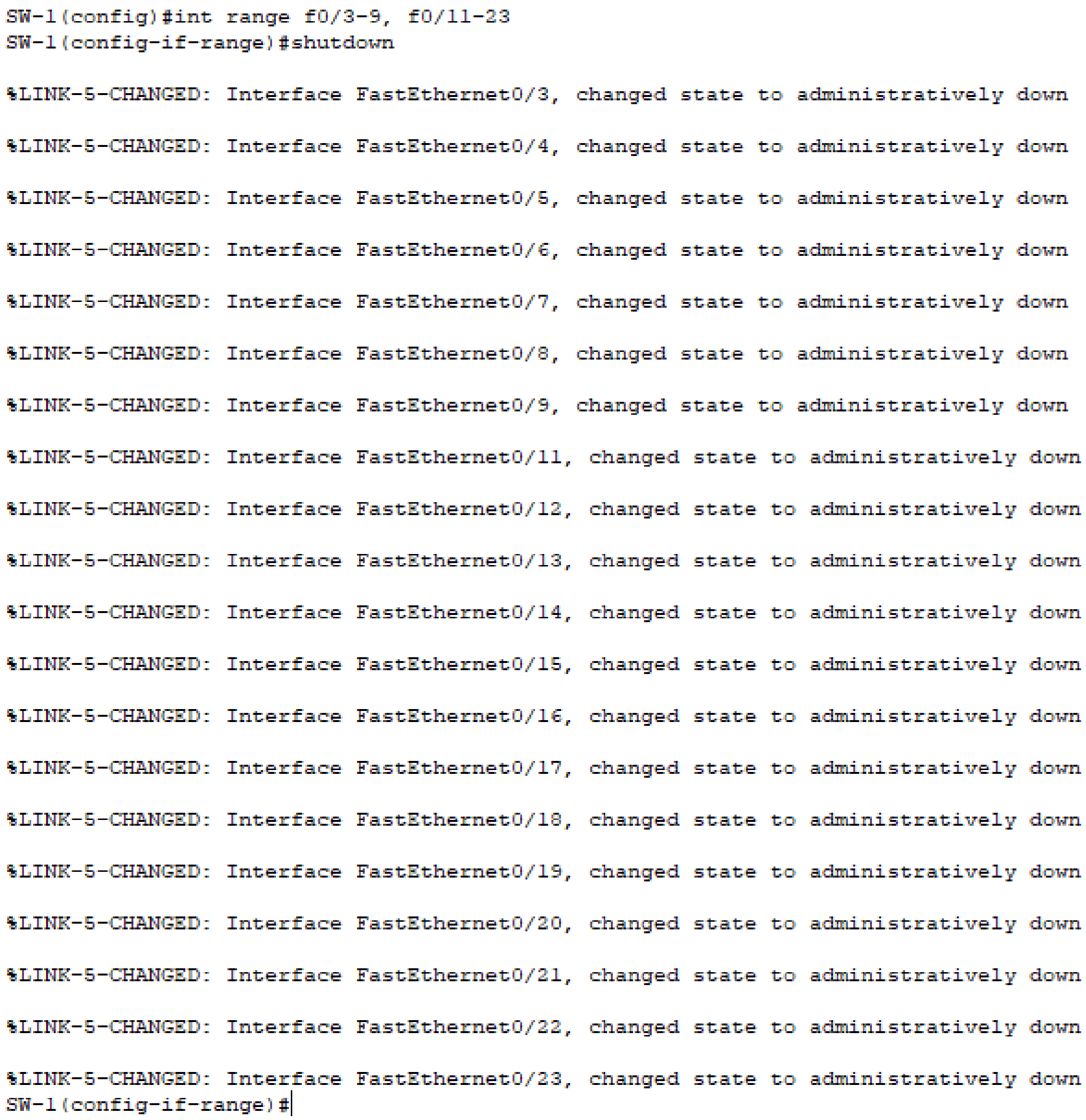
```
SW-2>en
SW-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-2(config)#int range g0/1-2
SW-2(config-if-range)#s
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (1), with DLS1 GigabitEthernet1/0/2 (100).
SW-2(config-if-range)#switchport mode trunk

SW-2(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

SW-2(config-if-range)#%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 100 on GigabitEthernet0/1 VLAN1.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking GigabitEthernet0/1 on VLAN0001. Inconsistent local vlan.


SW-2(config-if-range)#switchport nonegotiate
SW-2(config-if-range)#vlan 100
SW-2(config-vlan)#name Native
SW-2(config-vlan)#int range g0/1-2
SW-2(config-if-range)#switchport mode native vlan 100
                                      ^
% Invalid input detected at '^' marker.

SW-2(config-if-range)#switchport native vlan 100
                                  ^
% Invalid input detected at '^' marker.

SW-2(config-if-range)#switchport trunk native vlan 100
SW-2(config-if-range)#%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking GigabitEthernet0/1 on VLAN0100. Port consistency restored.

%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking GigabitEthernet0/1 on VLAN0001. Port consistency restored.
```

Step 2: Secure Unused Switchports

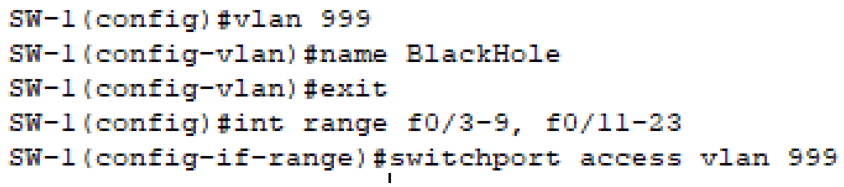
a. Shut down all unused switch ports on SW-1
b. On SW-1, create a VLAN 999 and name it BlackHole. The configured name must match the requirement exactly.
c. Move all unused switch ports to the BlackHole VLAN.

The following commands were used:

```
SW-1(config)#int range f0/3-9, f0/11-23
SW-1(config-if-range)#shutdown
SW-1(config)#vlan 999
SW-1(config-vlan)#name BlackHole
SW-1(config-vlan)#exit
SW-1(config)#int range f0/3-9, f0/11-23
SW-1(config-if-range)#switchport access vlan 999
```



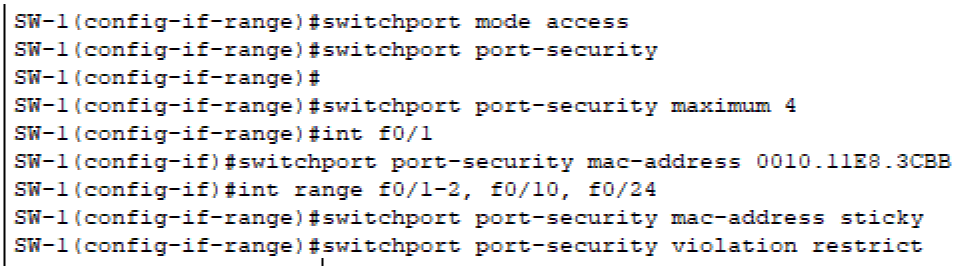
```
SW-1(config)#int range f0/3-9, f0/11-23
SW-1(config-if-range)#shutdown

%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 FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%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
SW-1(config-if-range)#
```



```
SW-1(config)#vlan 999
SW-1(config-vlan)#name BlackHole
SW-1(config-vlan)#exit
SW-1(config)#int range f0/3-9, f0/11-23
SW-1(config-if-range)#switchport access vlan 999
```

Step 3: Implement Port Security

a. Activate port security on all the active access ports on switch SW-1
b. Configure the active ports to allow a maximum of 4 MAC addresses to be learned on the ports.
c. For ports F0/1 on SW-1, statically configure the MAC address of the PC using port security.
d. Configure each active access port so that it will automatically add the MAC addresses learned on the port to the running configuration.



```
SW-1(config-if-range)#switchport mode access
SW-1(config-if-range)#switchport port-security
SW-1(config-if-range)#
SW-1(config-if-range)#switchport port-security maximum 4
SW-1(config-if-range)#int f0/1
SW-1(config-if)#switchport port-security mac-address 0010.11E8.3CBB
SW-1(config-if)#int range f0/1-2, f0/10, f0/24
SW-1(config-if-range)#switchport port-security mac-address sticky
SW-1(config-if-range)#switchport port-security violation restrict
```

Reflection Questions:

Task # 01:

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?
   Ans: Since sticky learning dynamically learns the MAC address and “sticks” them there is no need to put a remaining age for the timer.

2. In reference to Port Security, what is the difference between the absolute aging type and inactivity aging type?
   Ans: In the absolute aging type, the MAC addresses are removed after a specific amount of time expires, and this time of expiration doesn’t depend on any other factor. On the contrary, inactivity aging removes the MAC address after a specific amount of time *after the source device is inactive* i.e after there is no data frame coming from the source device.

   The inactivity timer starts after the device becomes inactive while the absolute timer starts from when it is set.

Challenges (if any):

- The concept of port security is interesting. I don’t think I faced any major challenges, and I improvised some sections which felt confusing. I’m interested in having upcoming labs cover other aspects of network vulnerability.

- For some reason, this command isn’t working on S1 in Task-1 Part-3 Step 4.

```
S1(config-if)#switchport port-security aging type inactivity
```