CSE 4512 [Computer Networks Lab]

Lab # 08

1. Objectives:

- Describe the concept of Switch Port Security
- Explain importance of Switch Port Security in securing an organization
- Configure Switch Port Security in CISCO devices
- Use Switch Port Security feature to achieve varying degrees of protection

2. Theory:

In this lab, you'll learn about **Switch Port Security**, one of the fundamental security mechanisms in Layer 2.

Switch Port Security:

At first, a word of caution. Don't confuse the ports that we'll discuss/secure here with the Application layer ports like port 80 (HTTP), 22 (SSH) etc. Those are at the topmost layer and implemented in *software* level. Switch ports are *hardware* ports in layer 2 of OSI model. You can connect a cable with these ports and then access the network.
One key aim of securing any infrastructure is to protect unauthorized physical access to the assets, its more important for digital assets. If any hacker/intruder gets physical access to the devices in an organization, then its *Game Over* for the company. Because its almost trivial for an experienced hacker to enter into the network and do catastrophic damage if physical access can be achieved.

One of the common ways to breach a network after gaining physical access is through the ports of the network switches. The intruder can connect his device through that port and as the ports are open to connect *by default*, he/she can then leverage various tools & techniques to attack the connected network. So, it should be pretty obvious by now as to why you need to learn the techniques of securing these vulnerable ports. Don't worry. This is not so difficult as there are commands & options available readily that you can use to protect the switch ports. Just you need to understand those options and use them according to your needs.
Before diving into the actual commands, let's first know what would be our ultimate objective here. As mentioned earlier, switch ports are in layer 2 that means in the MAC layer. So, if we can somehow specify the authorized MAC address and block access to any other MAC address then we can effectively secure the ports. The commands that you'll learn next will achieve this objective and also give you options for specifying various degrees of protection depending on your overall goal.

By default, switchport security feature is disabled. You have to enable it first by entering into a specific interface and then typing the command `switchport port-security` in the interface mode. Recall that, the interfaces are the actual ports in a CISCO device. Now if you try to execute the `switchport port-security` command directly then it'll be rejected. Its because the command can only be executed in a manually configured trunk or access port. But the ports are dynamic by

default. So, access/trunk mode needs to be enabled first in the port using the command `switchport mode {access | trunk}`.
After enabling switchport security feature, you can then specify different options for granular control over different protection mechanisms. The different available options are listed below:

```
S1(config-if)# switchport port-security ?
  aging         Port-security aging commands
  mac-address   Secure mac address
  maximum       Max secure addresses
  violation     Security violation mode <cr>
```

Limit and learn MAC addresses

To set the maximum number of MAC addresses allowed on a port, 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 depends 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 can be configured to learn about MAC addresses on a secure port in one of three ways:

1. Manually Configured

The administrator manually configures 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. Note that, the MAC addresses learnt 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 period.

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. Note that, 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` options. This options basically will tell what to do if any security violation 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.

A comparison of the three modes is given in the table below:

Violation Mode	Discards Offending Traffic	Sends Syslog Message	Increase Violation Counter	Shuts Down Port
Protect	Yes	No	No	No
Restrict	Yes	Yes	Yes	No
Shutdown	Yes	Yes	Yes	Yes

Verify port security

You can see the overall device-wide port security status by running the `show port-security` command in the privileged-exec mode.

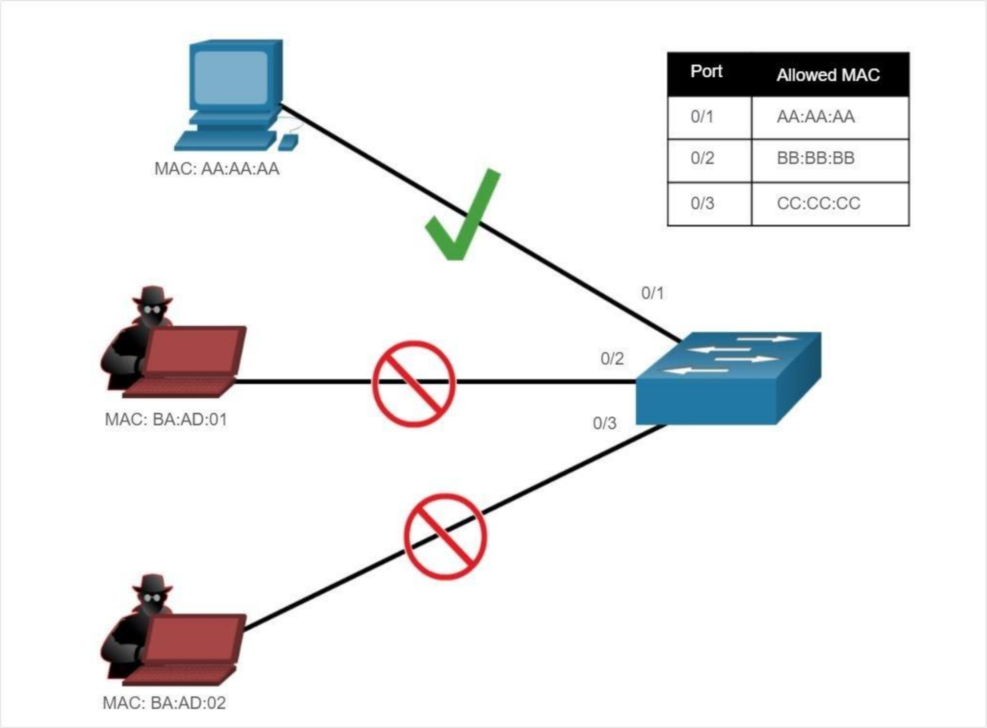
```
S1# show port-security
```

For the status of a specific port, following command is used.

```
S1# show port-security interface fastethernet 0/1
```

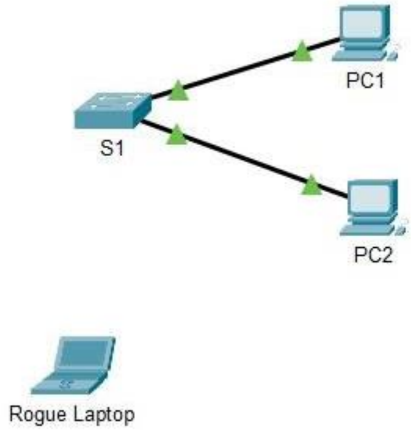
To see the allowed addresses in all the ports of the switch, following command is used in the privileged-exec mode.

```
S1# show port-security address
```



Port	Allowed MAC
0/1	AA:AA:AA
0/2	BB:BB:BB
0/3	CC:CC:CC

3. Configure Switch Port Security:



Step 1: Configure Port Security

a. Access the command line for **S1** and enable port security on Fast Ethernet ports 0/1 and 0/2.

```
S1(config)# interface range f0/1 - 2
S1(config-if-range)# switchport port-security
```

b. Set the maximum so that only one device can access the Fast Ethernet ports 0/1 and 0/2.

```
S1(config-if-range)# switchport port-security maximum 1
```

c. Secure the ports so that the MAC address of a device is dynamically learned and added to the running configuration.

```
S1(config-if-range)# switchport port-security mac-address sticky
```

d. Set the violation mode so that the Fast Ethernet ports 0/1 and 0/2 are not disabled when a violation occurs, but a notification of the security violation is generated and packets from the unknown source are dropped.

```
S1(config-if-range)# switchport port-security violation restrict
```

e. Disable all the remaining unused ports. Use the **range** keyword to apply this configuration to all the ports simultaneously.

```
S1(config-if-range)# interface range f0/3 - 24 , g0/1 - 2
S1(config-if-range)# shutdown
```

Step 2: Verify Port Security

a. From **PC1**, ping **PC2**.

b. Verify that port security is enabled and the MAC addresses of **PC1** and **PC2** were added to the running configuration.

```
S1# show run | begin interface
```

c. Use port-security show commands to display configuration information.

```
S1# show port-security
S1# show port-security address
```

d. Attach **Rogue Laptop** to any unused switch port and notice that the link lights are red.

e. Enable the port and verify that **Rogue Laptop** can ping **PC1** and **PC2**. After verification, shut down the port connected to **Rogue Laptop.**

f. Disconnect **PC2** and connect **Rogue Laptop** to F0/2, which is the port to which PC2 was originally connected. Verify that **Rogue Laptop** is unable to ping **PC1**.

g. Display the port security violations for the port to which **Rogue Laptop** is connected.

```
S1# show port-security interface f0/2
```

How many violations have occurred?

h. Disconnect **Rouge Laptop** and reconnect **PC2**. Verify **PC2** can ping **PC1**.

Why is **PC2** able to ping **PC1**, but the **Rouge Laptop** is not?

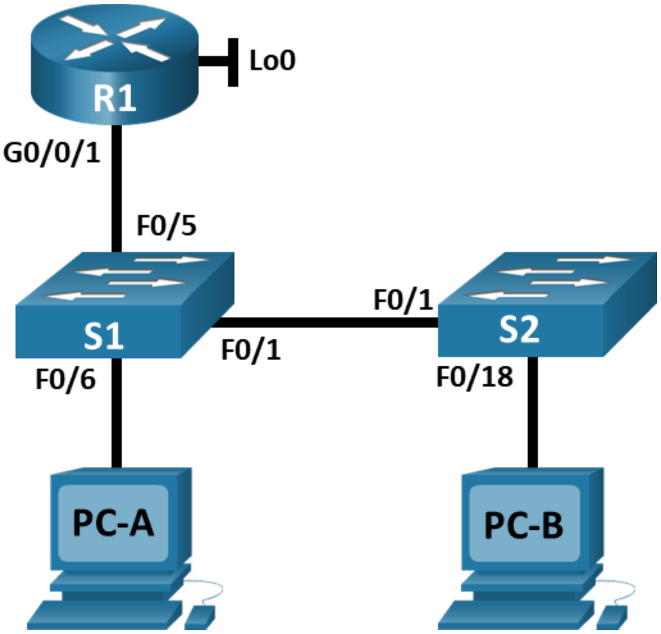
4. Tasks:

I. Implement the given network topology with the provided address specifications as described in the pdf ***Task-1_Port Security***. Configure *Switch Port Security* according to given instructions. Answer the questions accordingly. You're ***not*** provided a .pka file for this task. Make sure you've properly read on the *theory section of this handout* to understand the concepts mentioned.

II. Configure *Switch Port Security* according to the instructions given in the pdf ***Task-2_Port Security***. You're provided a .pka file for this task. As with task 1, make sure you've read on the theory section properly. Our suggestion would be to attempt task 2 after you've completed task 1 as many of the concepts of Switch Port Security is explained and shown in task 1.

Lab - Switch Security Configuration

Topology



Addressing Table

Device	Interface / VLAN	IP Address	Subnet Mask
R1	G0/0/1	192.168.10.1	255.255.255.0
R1	Loopback 0	10.10.1.1	255.255.255.0
S1	VLAN 10	192.168.10.201	255.255.255.0
S2	VLAN 10	192.168.10.202	255.255.255.0
PC – A	NIC	DHCP	255.255.255.0
PC – B	NIC	DHCP	255.255.255.0

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.
- Verify end-to-end-connectivity.

Background / Scenario

This is a comprehensive lab to review previously covered Layer 2 security features.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.3 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Make sure that the switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

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

Instructions

Part 1: Configure the Network Devices.

Step 1: Cable the network.

a. Cable the network as shown in the topology.

b. Initialize the devices.

Step 2: Configure R1 (follow network configuration table).

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.

Part 2: Configure VLANs on Switches.

Step 1: Configure VLAN 10.

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

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 provide a description for the interface.

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.

Part 3: Configure Switch Security.

Step 1: Implement 802.1Q trunking.

a. On both switches, configure trunking on F0/1 to use VLAN 333 as the native VLAN.

b. Verify that trunking is configured on both switches.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      333

Port        Vlans allowed on trunk
Fa0/1       1-4094

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       1-4094

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.

d. Verify with the **show interfaces** command.

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

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

Step 2: Configure access ports.

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

b. On S2, configure F0/18 as an access port that is associated with VLAN 10.

Step 3: Secure and disable unused switchports.

a. On S1 and S2, move the unused ports from VLAN 1 to VLAN 999 and disable the unused ports.

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

```
S1# show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1     Link to S2         connected    trunk      a-full  a-100 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         a-full  a-100 10/100BaseTX
Fa0/6     Link to PC-A       connected    10         a-full  a-100 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
<output omitted>
S2# show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1     Link to S1         connected    trunk      a-full  a-100 10/100BaseTX
Fa0/2                        disabled     999          auto   auto 10/100BaseTX
Fa0/3                        disabled     999          auto   auto 10/100BaseTX
<output omitted>
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         a-full  a-100 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
Gi0/1                         disabled     999          auto    auto 10/100/1000BaseTX
Gi0/2                         disabled     999          auto    auto 10/100/1000BaseTX
```

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.

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.

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

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

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

c. Verify port security on S1 F0/6.

```
S1# show port-security interface f0/6
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 60 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 3
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0022.5646.3411:10
```

```
Security Violation Count   : 0

S1# show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
10    0022.5646.3411    SecureDynamic                 Fa0/6       60 (I)
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

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.

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

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

f. Verify port security on S2 F0/18.

```
S2# show port-security interface f0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
Aging Time                 : 60 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0022.5646.3413:10
Security Violation Count   : 0

S2# show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                       (mins)
----    -----------       ----                          -----   -------------
10    0022.5646.3413    SecureSticky                  Fa0/18        -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

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.

Reflection Questions

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?

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

Packet Tracer - Switch Security Configuration

VLAN Table

Switch	VLAN Number	VLAN Name	Port Membership	Network
SW-1	10	Admin	F0/1, F0/2	192.168.10.0/24
	20	Sales	F0/10	192.168.20.0/24
	99	Management	F0/24	192.168.99.0/24
	100	Native	G0/1, G0/2	None
	999	BlackHole	All unused	None
SW-2	10	Admin	F0/1, F0/22	192.168.10.0/24
	20	Sales	F0/10	192.168.20.0/24
	99	Management	F0/24	192.168.99.0/24
	100	Native	None	None
	999	BlackHole	All unused	None

Objectives

Part 1: Create a Secure Trunk

Part 2: Secure Unused Switchports

Part 3: Implement Port Security

Background

You are enhancing security on two access switches in a partially configured network. You will implement the range of security measures that were covered in this module according to the requirements below. Note that routing has been configured on this network, so connectivity between hosts on different VLANs should function when completed.

Instructions

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.

Step 2: Secure Unused Switchports.

a. Shutdown 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.

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.

e. Configure the port security violation mode to drop packets from MAC addresses that exceed the maximum, generate a Syslog entry, but not disable the ports.