CSE 4412 [Data Communication and Networking Lab]

Lab # 06

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
- Describe the concept of port mirroring
- Implement port mirroring using Cisco Switch Port Analyzer (SPAN)
- Explain use cases of SPAN in real-life

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 at the *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, the 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. However, 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` option. This option basically will tell what to do if any security violation occurs. 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.

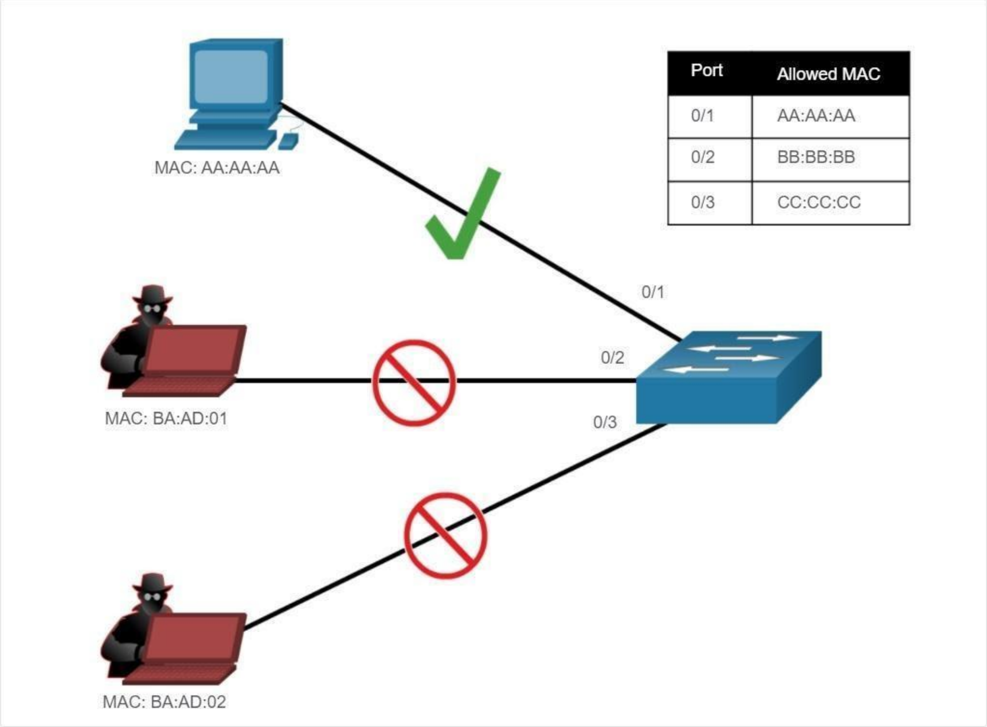
```
S1# show port-security
```

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

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

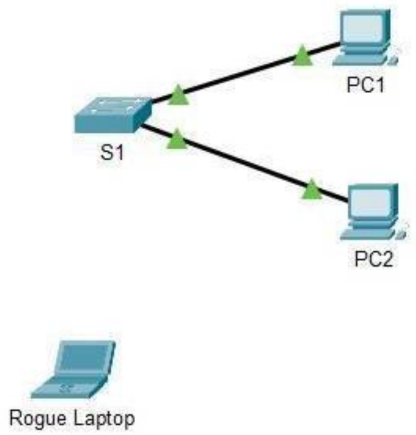
To see the allowed addresses in all the ports of the switch, following command is used in the privileged-exec mode.

```
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?

Switch Port Analyzer:

One day your boss called you and asked you to monitor if your colleagues are using Facebook during office hours. How do you do it? Or you've been informed of an ongoing cyber attack on your office hosts. How do you know what attacker is doing? All of these and more can be achieved through a CISCO feature known as SPAN or Switch Port Analyzer. SPAN is a port mirroring technique that allows administrators or devices to collect and analyze traffic.

What is this port mirroring, actually? The name tells the tale. It mirrors traffic from one port to another port. The packets from one port are copied and sent to another port, where a packet analyzer is connected. This packet analyzer can be a purpose-built hardware or it can be an application like Wireshark or an Intrusion Detection System (IDS) running on a host device. Technically, these are Ethernet frames which will be mirrored.

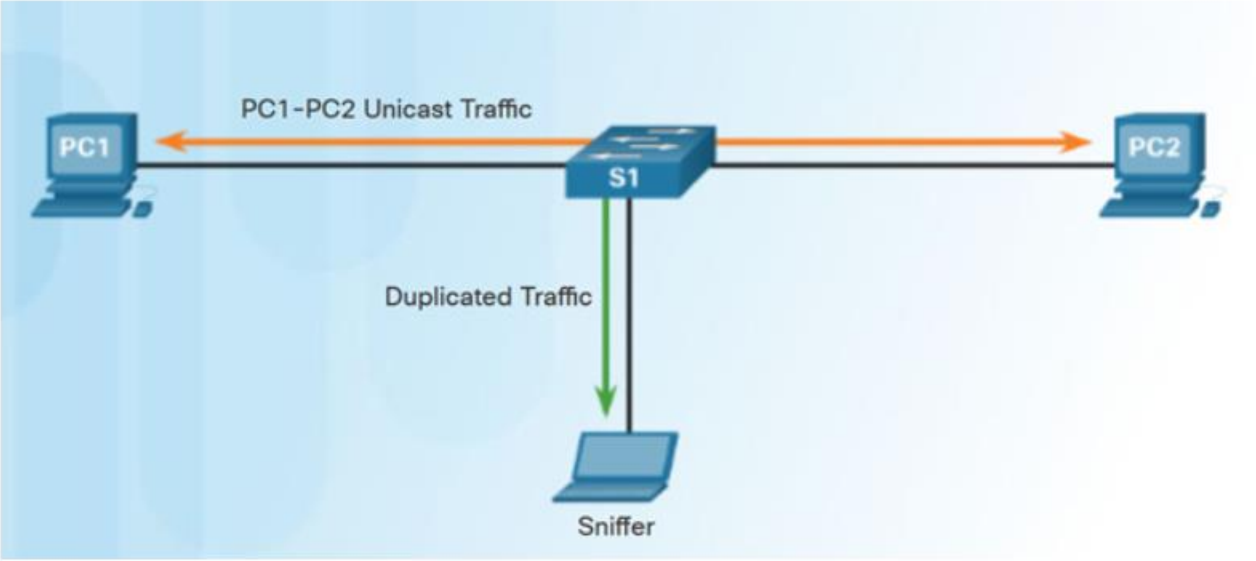


Fig: Port Mirroring

The specific technology that allows this port mirroring in Cisco devices is known as SPAN. There are two types of SPAN: Local SPAN and Remote SPAN. When traffic on a switch port is mirrored to another port on that switch, then it's *Local SPAN*. In contrast, when traffic is mirrored to a port on another switch then it's *Remote SPAN*. In this lab, we'll focus only on Local SPAN.

When configuring SPAN, an association between the *source ports* (the port whose traffic would be copied/mirrored) and the *destination port* (the port through which the copied/mirrored traffic will be sent) is made. In SPAN terminology, this association is known as a *session*. You can mirror traffic from multiple source ports or from a source VLAN to a single destination port. The destination port is also known as the monitor port. Note that, a destination port can't be a source port or a source port can't be a destination port. It depends on the specific Cisco device and the number of destination ports that can be there for a single session. And when you configure a normal port as a *destination port*, only mirrored/monitored traffic can pass through it. Other traffic will no longer be able to pass through that port.
There are some other related terminologies in SPAN. The traffic that enters a switch port is called ingress traffic and the traffic that leaves through a switch port is known as egress traffic. The traffic onto a source port can be mirrored/monitored in either ingress or egress mode or in both directions. By default, both ingress and egress traffic are mirrored to the specified destination ports.

Configuration of SPAN is pretty easy. Only a single command format is used. You just have to specify the correct pair of source and destination ports and the mirroring would be enabled in no time. The following two commands are used for enabling SPAN:

```
S1(config)# monitor session 1 source interface f0/5
S1(config)# monitor session 1 destination interface f0/6
```

Here, 1 is the session ID. Each pair of pair of source and destination would belong to a separate session.

Verify using:

```
S1# show monitor
```

4. Tasks:

Make sure you've properly read the *theory section of this handout* to understand the concepts mentioned.

X = Last 2 digits of your Student ID
Z = Last digit of your Student ID

I. Implement 2 VLANs on each of the two switches, namely admin and student in the first switch, and student and teacher in the second switch. The VLANs should be 192.168.X+1.0 and 192.168.X+7.0. Use Router-on-a-stick or L3 switch (whichever you prefer) to support Inter-VLAN communication. Now, configure port security on the switches. Of the 4 ports (2 from each switch), make 1 port as

Protect, 2 ports as Restrict and 1 port as Shutdown. Disconnect one of the current PCs and use a rogue PC to communicate with other PCs. Keep doing this until the count for restrict is Z.

II. Configure SPAN on the port where students are connected so that any communication they make are reported to the admin.