Khwopa College of Engineering
Libali, Bhaktapur
Department of Computer Engineering

Computer Network (CT 657)

LAB 8

Port Security on Switch

Objective:

1. To configure, verify, and troubleshoot port security on switch.

Aparatus: Packet Tracer

Theory

- Layer 2 Switching is the process of using the hardware address of devices on a LAN to segment a network.
- A switch breaks up a large collision domains into smaller ones and that a collision domain is a network segment with two or more devices sharing the same bandwidth. Each port on a switch is actually its own collision domain.
- Switch uses application specific integrated cirucits (ASICs) to build and maintain their MAC filter tables.
- A switch is a multiport bridge as it break up collision domain
- Layer 2 switches and bridges are faster than routers because they don't take up time looking at the Network layer header information. Instead, they look at the frame's hardware addresses before deciding to either forward, flood, or drop the frame.
- Unlike hubs, switches create private, dedicated collision domains and provide independent bandwidth exclusive on each port.
- Here's a list of four important advantages we gain when using Layer 2 switching:
  - Hardware-based bridging (ASICs)
  - Wire speed
  - Low latency
  - Low cost

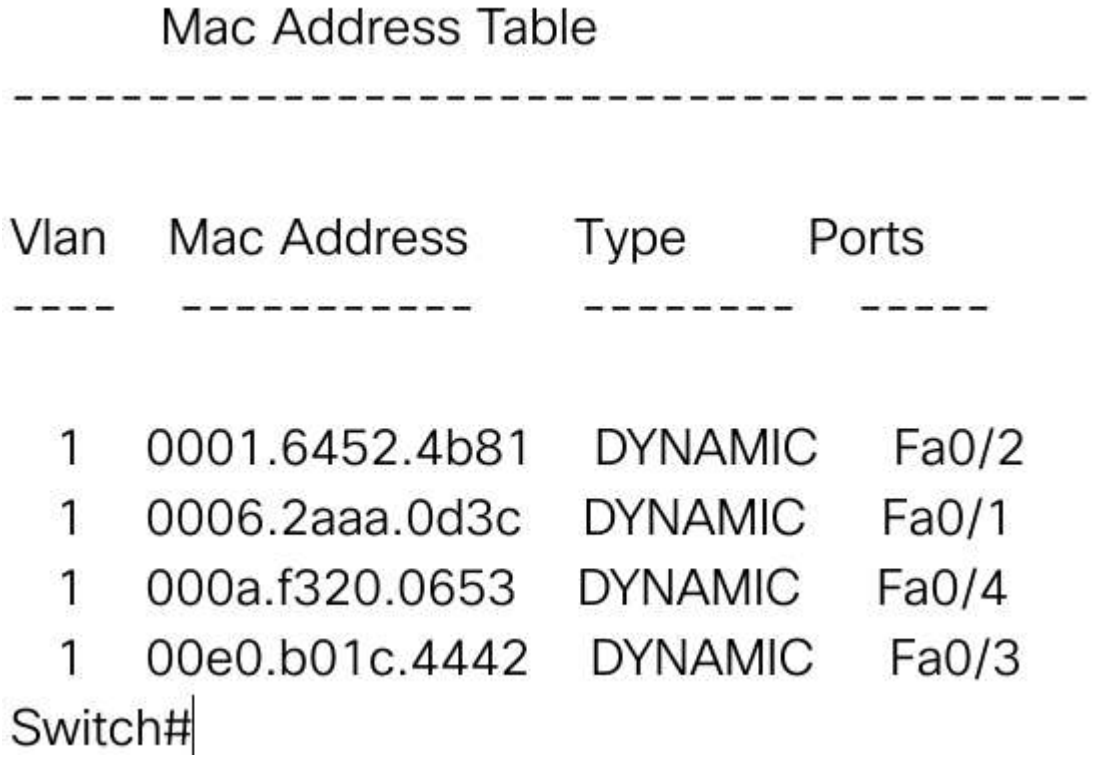
Three Switch Function at Layer 2

Address learning Layer 2 switches remember the source hardware address of each frame received on an interface and enter this information into a MAC database called a forward/filter table.

Forward/filter decisions When a frame is received on an interface, the switch looks at the destination hardware address, then chooses the appropriate exit interface for it in the MAC database. This way, the frame is only forwarded out of the correct destination port.

Loop avoidance If multiple connections between switches are created for redundancy purposes, network loops can occur. Spanning Tree Protocol (STP) is used to prevent network loops while still permitting redundancy.

Task 1: Showing MAC address table in switch
Switch>enable
Switch#show mac address-table



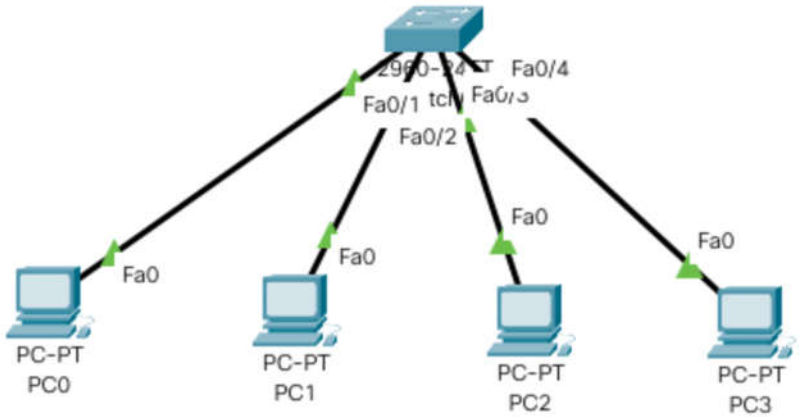


Figure 1: Four hosts connected to the a switch.

Port Security

- It's usually not good thing to have your switches available for anyone to just plug into an play around with.
- We need to prevent someone from simply plugging a host into one of switch ports.
- Be default, MAC addresses will just dynamically appear in your MAC forward/filter database and you can stop them in their tracks by using port security.
- By using port security, we can limit the number of MAC addresses that can be assigned dynamically to a port, set static MAC addresses, or set penalties for users who violate the policy.

Configuring port security

Swtich>**enable**
Switch#**Config t**
Switch(config)# i**nt f0/1**
Swtich(config-if)#**swithcport mode access**
Switch(config-if)#**switchport port-security**
Switch(config-if)#**switchport port-security ?**

```
Aging              Port-security aging commands
mac-address              Secure mac address
maximum            Max secure addresses
violation          Security violation mode
< cr >
```

If you want to set up a switch port to allow only one host per port and make sure the port will shut down if this rule is violated, use the following commands like this:

Switch(config-if)#**switchport port-security maximum 1**
Switch(config-if)#**switchport port-security violation shutdown**

The drawback to this is that it only allows a single MAC address to be used on the port, so if anyone, including you, tries to add another host on that segment, the switch port will immediately shut down. And when that happens, you have to manually go into the switch and re-enable the port by cycling it with a *shutdown* and then a *no shutdown command.*

Alternatively we can use *sticky* command.

Switch(config-if)#**switchport port-security mac-address sticky**
Switch(config-if)#s**witchport port-security maximum 2**
Switch(config-if)#**switchport port-security violation shutdown**

Here, the first two MAC addresses coming into the port "stick" to it as static addresses and will be placed in the *running-config*, but when a third address tried to connect, the port would shut down immediately.

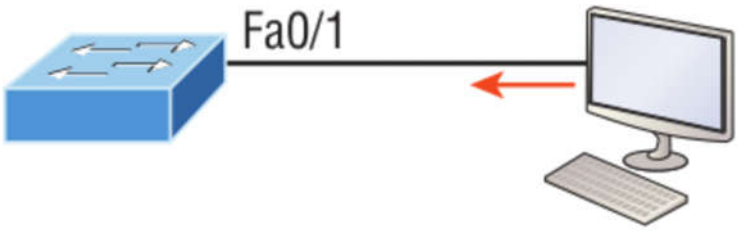


Figure 2: Protecting a lobby PC.

When we want to need to be secured against the Ethernet cable used by anyone other than a single authorized individual.

Switch(config-if)#**switchport port-security**
Switch(config-if)#**switchport port-security violation restrict**
Switch(config-if)#**switchport port-security mac-address aa.bb.cc.dd.ee.ff**

To protect the lobby PC, we would set the maximum allowed MAC addresses to 1 and the violation to restrict so the port didn't get shut down every time someone tried to use the Ethernet cable (which would be constantly). By using violation restrict , the unauthorized frames would just be dropped. But did you notice that I enabled port-security and then set a static MAC address? Remember that as soon as you enable port-security on a port, it defaults to violation shutdown and a maximum of 1. So all I needed to do was change the violation mode and add the static MAC address and our business requirement is solidly met!

To verify port security
Switch# show port-security int f0/1