PORT SECURITY AND CONFIGURATION

Switch port security limits the number of valid MAC addresses allowed on a port. When a MAC address, or a group of MAC addresses are configured to enable switch port security, **the switch will forward packets only to the devices using those MAC addresses.** Any packet coming from other device is discarded by the switch as soon as it arrives on the switch port.

I**f you limit the number of allowed MAC addresses allowed on a port to only one MAC address, only one device will be able to connect to that port and will get the full bandwidth of the port.**

If the maximum **number of secure MAC addresses has been reached, a security violation occurs** when a device with a different MAC address tries to attach to that port. In most of today's scenarios when the switch detects a security violation, the switch automatically shuts down that port.

#**A switch can be configured to only protect or restrict that port**. We will discuss these security violation modes a little bit later.

Secure MAC addresses are of three types:

- **Static secure MAC addresses** – configured manually with **switchport port-security mac-address *mac-address***. These MAC addresses are stored in the address table and in the running configuration of the switch.
- **Dynamic secure MAC addresses** – are dynamically learned by the switch and stored in its MAC address table. They are removed from the configuration when the switch restarts.
- **Sticky secure MAC addresses** – like Dynamic secure MAC addresses, MACs are learned dynamically but are saved in the running configuration.

Sticky secure MAC addresses have these characteristics:

- Are learned dynamically then converted to sticky secure MAC addresses and stored in the running configuration.
- **When you disable the sticky learning, the learned addresses remain part of the MAC address table but are removed from the configuration.**
- When you disable port security, the sticky secure MAC addresses remain in the running configuration.
- If you save the addresses in the configuration file, when a restarts or the interface shuts down, the switch does not need to relearn the addresses.

In a Cisco switch, you are able to configure three types of **security violation modes**. A security violation occurs when the maximum number of MAC addresses has been reached and a new device, whose MAC address is not in the address table attempts to connect to the interface or when a learned MAC address on an interface is seen on another secure interface in the same VLAN.

Depending on the action you want a switch to take when a **security violation** occurs, you can configure the behavior of a switch port to one of the following:

- **protect** – when the maximum number of secure MAC addresses has been reached, **packets from devices with unknown source addresses are dropped** until you remove the

necessary number of secure MAC addresses from the table. In this mode, you are not notified when a security violation occurs.

- **restrict** – is identical with protect mode, but notifies you when a security violation occurs. Specifically, a SNMP trap is sent, a syslog message is logged and the violation counter increments.
- **shutdown** – **this is the default behavior on a switch**. In this mode, the **switch ports shuts down when the violation occurs**. Also, a SNMP trap is sent and the message is logged. You can enable the port again with the **no shutdown** interface configuration command.

The default configuration of a Cisco switch has port security disabled. If you enable switch port security, the default behavior is to allow only 1 MAC address, shutdown the port in case of security

CONFIGURATION

violation and sticky address learning is disabled.

Next, we will enable dynamic port security on a switch.

Switch(config)**#interface FastEthernet 0/1**

Switch(config-if)**#switchport mode access**

Switch(config-if)**#switchport port-security**

As you can see, we did not specify an action to be taken if a security violation occurs, neither how many MAC addresses are allowed on the port. Recalling from above, the default behavior is to shutdown the port and allow only one MAC address.

Let's now configure a sticky port security, to allow 10 MAC addresses on the interface. If a violation occurs, you want the port to be configured in restrict mode.

Switch(config)**#interface FastEthernet 0/1**

Switch(config-if)**#switchport mode access**

Switch(config-if)**#switchport port-security**

Switch(config)if)**#switchport port-security maximum 10**

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

Switch(config-if)**#switchport port-security violation restrict**

Good. After you have configured port security in the desired mode on a switch, it's time to verify the configuration and the learned MAC addresses with the **show port-security interface *interface-id*** and with **show port-security address**.

Switch**#show port-security interface FastEthernet 0/1**

Port Security : Enabled

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 : 1

Configured MAC Addresses : 0

Sticky MAC Addresses : 0

Last Source Address:Vlan : 0000.0000.0000:0

Security Violation Count : 0

Switch**#show port-security address**

Secure Mac Address Table

———————————————————————-

Vlan Mac Address Type Ports Remaining Age

(mins)

—- ——— —- ——— ———-

11 0050.BAA6.0001 SecureDynamic Fa0/1 –

Total Addresses in System: 0
Max Addresses limit in System: 8320

Now, you may wonder what to do with an unused interface. Securing an unused interface is important too and it's much simpler. The only thing you have to do is to put all unused interfaces in shutdown state with the **shutdown** interface configuration command.
Switch(config)**#interface FastEthernet 0/2**

Switch(config-if)#**shutdown**