9(B). Switch Port Security

Port Security—restricts switchports to only pass frames with the expected source MAC address(es). Port security can even be applied to a trunk switchport to filter a large chunk of a network.

Violation Responses

Violation Mode	Effect
Protect	Drop frames whose source MAC address isn't expected.
Restrict	Add logging to the response and increment the interface error count
Shutdown	(Default) All of the above, plus put the interface in err-disabled mode, shutting down all traffic on the port until an administrator fixes it.

```
SW(config-if)# switchport port-security
```
Turns on port security
```
SW(config-if)# switchport port-security maximum 3
```
Maximum number of unique MAC addresses Allowed (Default 1)
```
SW(config-if)# switchport port-security mac-address 1234.5678.90ab
```
Manually define (one of) the allowed MAC address(es)
```
SW(config-if)# switchport port-security mac-address sticky
```
Allow the switch to automatically put a mac-address line, similar to the one above, in the running config to match whatever source MAC address it hears. It will continue adding such lines until it reaches the maximum, then it'll enforce. For the resulting auto config to survive restarts, you'll need to copy running-config to startup-config after it has learned.
```
SW(config-if)# switchport port-security mac-address sticky 1245.6789.0abc
```
This is what that automatically added line would look like in the running-config after it learned an address. Notice that it keeps the word "sticky" and adds a mac address. Also, this line doesn't replace the sticky line above, it just gets added as a separate line.
```
SW(config-if)# switchport port-security violation { protect | restrict | shutdown }
```
Default = shutdown