Switch# show port-security

Note that the violation count is incremented ONLY because the mode is restrict or shutdown. In mode "protect," there would be no log messages and no violation count! It would show Max 1, Current 1, Violations 0, Action Protect.

```
S1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
     Fa0/13            1           1                 37         Restrict
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 5120
```

Switch# show port-security interface fa0/13

Port status tells us the actual state of the interface; violation mode tells us what it *would* be if there were a violation. Remember that the port status will only change in response to a violation if the violation mode is "shutdown." In both protect and restrict modes, frames from non-allowed mac addresses will be blocked, but the port won't change status. TODO: check if the "last source address" line updates in protect mode, since no logging is done in that mode.

```
S1#show port-security interface fa0/13
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000f.8f4b.b4a0:1
Security Violation Count   : 37
```

Switch# show running-config interface fa0/13

```
S1#show run interf fa0/13
Building configuration...

Current configuration : 182 bytes
!
interface FastEthernet0/13
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 0200.1111.1111
end
```

Switch# show mac address-table dynamic

Note that the address in the mac address-table for fa0/13 IS the manually entered one. Still no evidence of incorrect config if violation mode is "protect." NOTE: Ths book insists that the "switchport port-security mac-address …" MAC address would be listed as a static entry in the mac-address table, still used for routing, but filtered out if the "dynamic" keyword was used as shown. On a 3550 it shows up as dynamic (yellow line). TODO: check if the MAC shows as dynamic because frames with that MAC actually passed through. The book uses the example of a sticky-learned MAC to say that even though that had passed through, it wouldn't show up as dynamic. Perhaps newer switches than mine behave as the book suggests. Or, perhaps I'm seeing a side-effect of the 3550 being a layer 3 switch.

```
S1#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    000d.29a1.868b    DYNAMIC     Fa0/11
   1    000d.29a1.868c    DYNAMIC     Fa0/12
   1    000d.29f3.f387    DYNAMIC     Fa0/7
   1    000d.29f3.f388    DYNAMIC     Fa0/8
   1    000d.6520.2f89    DYNAMIC     Fa0/9
   1    000d.6520.2f8a    DYNAMIC     Fa0/10
   1    000f.8f22.a340    DYNAMIC     Fa0/17
   1    000f.8f22.a341    DYNAMIC     Fa0/18
   1    000f.8f4b.b4a1    DYNAMIC     Fa0/14
   1    0200.1111.1111    DYNAMIC     Fa0/13
Total Mac Addresses for this criterion: 10
```

Switch# show mac adress-table secure [interface fa0/1]

According to the book, this command *would* show the configured secure MAC address, not because it had passed through, but because it was configured as a secure address for the port.

Switch# debug port-security

Even this shows nothing in "protect" mode !!!

```
S1#debug port-security
All Port Security debugging is on
S1#
```

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

Changing the violation mode is the only way to demonstrate the problem and learn the MAC address of the actual device causing the violations.

```
S1(config)#interface fa0/13
S1(config-if)#switchport port-security violation restrict
S1(config-if)#
*Mar  1 01:10:27.195: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation
occurred, caused by MAC address 000f.8f4b.b4a0 on port FastEthernet0/13.
```

Switch# show interfaces status

Notice the status of err-disabled on fa0/20. That's what this command calls secure-down.

```
ernestine# show interfaces status

Port      Name                Status        Vlan       Duplex  Speed Type
...
Fa0/12    LJ5MP               connected     2          a-full  a-100 10/100BaseTX
Fa0/13    N/C Apartment West disabled      2            auto   auto 10/100BaseTX
Fa0/14    BLUFFER2            connected     2          a-full  a-100 10/100BaseTX
Fa0/15    Apartment North     notconnect    2            auto   auto 10/100BaseTX
...
Fa0/20    LJ8550dn            err-disabled 2            auto   auto 10/100BaseTX
```

Switch# show interfaces description

No fancy terminology here; it's just "down/down." That's no different than fa0/15, which doesn't have anything plugged in.

```
ernestine# show interfaces description
Interface                      Status         Protocol Description
...
Fa0/12                         up             up       LJ5MP
Fa0/13                         admin down     down     N/C Apartment West
Fa0/14                         up             up       BLUFFER2
Fa0/15                         down           down     Apartment North
...
Fa0/20                         down           down     LJ8550dn
```

Switch# show interfaces fa0/20

```
ernestine# show interfaces fa0/20
FastEthernet0/20 is down, line protocol is down (err-disabled)
...
```