Port Security

Port Security

- Used to limit access to a port based on MAC address or quantity of connected devices
- Can be configured on static access and trunk ports (but not "dynamic" ports)
- A secure port cannot be:
  - Destination port for SPAN
  - Port-channel
  - Private VLAN port

Port Security Violation Modes

- Shutdown
  - Disables the port by placing it in err-disable state
  - Generates an SNMP trap and syslog message
- Protect
  - Does not accept traffic from new device after violation occurs
- Restrict
  - Works just like protect mode and generates SNMP and syslog

Implementing Port Security

- Enabling port security
  - Switch(config-if)# switchport port-security
- Limiting number of MAC addresses
  - Switch(config-if)# switchport port-security maximum <number>
  - Switch(config-if)# switchport port-security mac-address <MAC> <sticky>

Implementing Port Security Violation Mode

- Setting violation mode
  - Switch(config-if)# switchport port-security violation <protect | restrict | shutdown>

Implementing Port Security

- Configuring recovery interval
  - Switch(config)# errdisable recovery psecure-violation
  - Switch(config)# errdisable recovery interval <interval in sec>

Port-Security (cont.)

- Applies to access and trunk ports, but not dynamic
  - Ensure port mode is statically defined
- Secure MAC addresses
  - Can only belong to one port
  - Static
  - Learned (dynamic)
  - Sticky
- Trunk ports
  - Support per-VLAN limits (default unlimited)
  - Port limit is aggregate across all VLANs

Port-Security (cont.)

- Remember that you can change device MACs
- Keep in mind port-security and HSRP interaction
  - HSRP/VRRP/GLBP add virtual MACs
  - Two solutions
    - Standby use-bia
    - Allowing the virtual MAC
- Avoid using "protected" mode on trunks
  - Disables MAC learning once limit is reached for any VLAN
- Consider additional MACs with IP Phones

1. Required, especially if BYOD are allowed on the network.
2. To avoid users plugging in rogue (APs, DHCPs, Raspberry pie (macof on Kali linux) etc.) to the network.
3. Protect from MAC Flooding. When someone starts generating bogus MAC addresses the switch can only hold a limited amount in its CAM table (MAC address table).
Once it's full it won't learn any new MAC addresses and as a result it will flood traffic. The attacker can run wireshark and try to capture some of the traffic of legitimate devices that is being flooded.

Protect: Ethernet frames from MAC addresses that are not allowed will be dropped but you won't receive any logging information.
Restrict: Ethernet frames from MAC addresses that are not allowed will be dropped but you will see logging information and a SNMP trap is sent.
Shutdown: Ethernet frames from MAC addresses that are not allowed will cause the interface to go to err-disable state. You will see logging information and a SNMP trap is sent. For recovery you have two options:

- Manual: The default aging time is 0 mins so you'll have to enable the interface yourself.
- Automatic: Configure the aging time to another value.

Configuration:

SW(config)#interface fa0/1
SW(config-if)#switchport mode access !(works only on access ports not on dynamic interfaces)
!(it can be configured on a trunk port, but not a good idea as the max MACs need to be set)

SW(config-if)#switchport port-security !(turn ON port security)
SW(config-if)#switchport port-security violation shutdown !(options: shutdown | protect | restrict) !(default is shutdown)
SW(config-if)#switchport port-security maximum 1 !(allows max 1 MAC address on the port) !(default max is 1)!(you might need max 2 MAC allowed if PC connected to Iphone and Iphone connected to switch)
SW(config-if)#switchport port-security mac-address aaaa.bbbb.cccc !(can hard code the allowed MAC)
OR
SW(config-if)#switchport port-security mac-address sticky !(or to get the MACs the switch sees instead of manually adding them, based on max MACs value set)

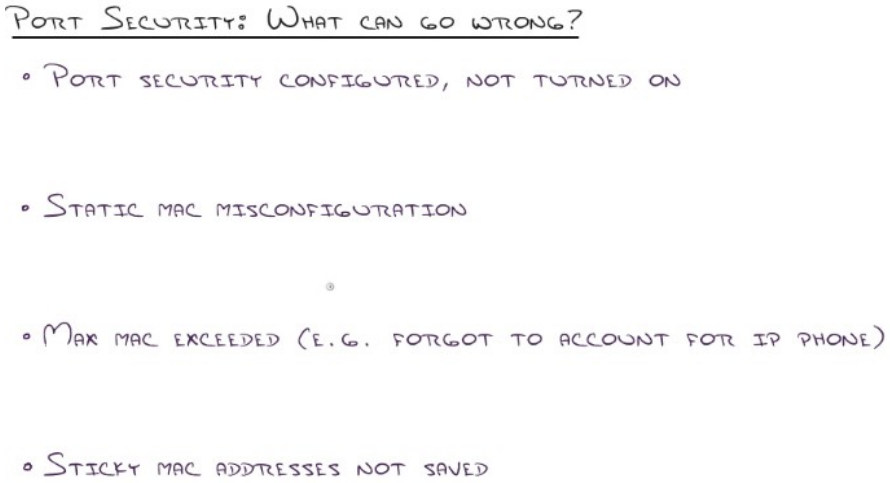
To bring the port manually up when it is in err-disable state, otherwise it will stay in it forever:

SW(config)#interface fa0/1
SW(config-if)#shutdown
SW(config-if)#no shutdown

To automatically bring the port up when it is in err-disable state:

SW(config)#errdisable recovery cause psecure-violation !(only when port security violation occurs)
SW(config)#interface fa0/1
SW(config-if)#switchport port-security aging time 10 !(in mins)!(default is 5 mins)

Verification and TSHOOT:



Check if an interface is in err-disabled and if so:
A) check why this happened and B) solve the problem.

sh port-security
sh port-security interface fa0/1 !(important)
sh port-security address
sh interfaces fa0/1
sh int status err-disable
sh err-disable recovery
sh mac-address-table
sh mac-address-table count
sh run