Port Security

What source MAC addresses a well as how many MAC addresses are allowed on a switch port.
Actions can be taken if an unauthorized src MAC address enters the port as err-disabled state.
One MAC address is allowed, if not configured manually, the first src MAC address entering the interface is allowed, yet the maximum number of MAC addresses allowed can be changed.
The switch's MAC address table can be full making it flood every packet it receives.
Can protect against DHCP starvation attack by limiting number of MAC addresses.
Port security can only be enabled on statically configured access/trunk ports.
If a MAC address is dynamically learned its cleared if the interface is err-disabled, if configured no.
Command: switchport port-security. Show port-security interface <interface name>.
To re-enable the interface disconnect the unauthorized device , shutdown and then no shutdown the interface.
Command: show errdisable recovery. Default timer is 300 seconds.
Command: errdisable recovery cause psecure-violation. Command: errdisable recovery interval <time>.
Shutdown: generates a syslog, snmp message when the interface is disabled, after the interface is down no messages are sent, violation count is set to 1 when disabled ad reset to 0 when enabled.
Restrict: the switch discards traffic from unauthorized MAC addresses, the interface is not disabled, violation counter is incremented by 1 for each unauthorized frame, a syslog/snmp message is generated each time an unauthorized MAC is detected.
Protect: just like restrict but silently discards the unauthorized traffic with no syslog/snmp messages, not increment violation counter.
Command: switchport port-security mac-address <mac>.
Command: switchport port-security violation restrict/protect/shutdown.
Command: switchport port-security aging time <minutes>.
Absolute: the counter goes down even if frames are consistently received during countdown.
Inactivity: the timer is reset with every frame received from the allowed MAC-addresses.
Command: switchport port-security aging type {absolute | inactivity}.
By default only dynamic MAC addresses age out, to make configured MAC addresses age too use:
Command: switchport port-security aging static. Command: show port-security.
Command: switchport port-security mac-address sticky.
When enabled all current dynamically learned MAC addresses will be converted to sticky, added to running-config, never age out, when disabled all sticky secure MAC addresses will be converted to regular dynamically-learned.
Sticky,static have a type of static,dynamically will have a type of dynamic**.**
Command: show mac-address table secure.
Command: switchport port-security maximum <max addresses>.