Port Security - 1

Port Security limits the number of MAC addresses the switch can learn on each interface.

Types of secure MAC addresses:

- Static secure MAC addresses: manually configured MAC addresses that are stored in the MAC address table, and added to the Switch running configuration and saved after a restart.
- Dynamic secure MAC addresses: dynamically learned MAC addresses, stored only in the address table, and removed when the Switch restarts.
- Sticky secure MAC addresses: dynamically learned or manually configured, stored in the address table, and added to the running configuration so they are also available after the switch restarts.

Port Security - 2

When the maximum number of secure MAC addresses have been reached a security violation occurs.

The switch can react to a security violation in three different ways:

- protect: packets with unknown source MAC addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowed addresses. There is no notification that a security violation has occurred.
- restrict: packets with unknown source MAC addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. A notification of type SNMP trap is sent, a syslog message is logged, and the violation counter increments.
- shutdown: the interface to immediately become error-disabled. It also sends an SNMP trap, logs a syslog message, and increments the violation counter. When a secure port is in the error-disabled state, one way you can bring it out of this state is by manually re-enable it by entering the *shutdown* and *no shutdown* interface configuration commands. This is the default mode.