Switch Port Security

The Switch Port Security concept allows protecting switch from connecting unauthorized devices. It allows to set the maximum number of MAC addresses per port, specify certain MAC addresses, etc.

Possibilities

Static:

Assign a specific MAC address to a specific port. Only devices with this address can connect to this port.

```
interface f0/1
       switchport mode access                          // usually not necessary
       switchport port-security                        // turn it on, enable port security
       switchport port-security mac-address xxxxxxx    // set the MAC address
```

Sticky:

After setting up, it remembers the MAC addresses of the first N connected devices, only those can connect.

```
interface f0/1
       switchport mode access                          // usually not necessary
       switchport port-security                        // turn it on
       switchport port-security maximum N              // set max. number of MAC addresses
       swidthport port-security mac-address sticky

show port-security interface xxxxx
```

Disabling port-security settings

```
interface f0/1
       no switchport port-security                     // turn it on off
```

Violation Modes

Security violation determines the behavior of the port when an unauthorized device attempts to connect.

Mode	Forwards frames from non-permitted MAC address	Forwards frames from allowed MAC addresses	Syslog report	Reporting error	Increases number of errors	Disable the port (error-disable state)
Protect	no	yes	no	no	no	no
Restrict	no	yes	yes	SNMP trap	yes	no
Shutdown	no	no	no	SNMP trap	yes	yes

Protect: if I connect a device with a non-permitted address, all traffic is dropped. For other devices, everything works. Nothing is reported to admin, nothing is logged.

Restrict: if I connect a device with a non-permitted address, all traffic is dropped and the counter for the number of non-permitted MAC addresses used is increased. For other devices everything works. Admin gets a report via SNMP trap, the event is forwarded to Syslog.

Shutdown (dafault value): if I connect a device with a non-permitted address, the device goes to the error-disabled state, does not working, the counter for the number of non-permitted MAC addresses used is increased. Admin gets a report via SNMP trap, the port needs to be made functional.

Example of setting the second option:

```
switchport port-security violation restrict
```

When the port has been disabled:

```
int xxxxx
       shutdown
       no shutdown
```