17. Port security on access layer switchport

Port security is feature that enable permit or deny traffic for end user PCs connected to access layer switch. Port security enable specify a group of valid MAC address on port. If maximum secure MAC address is reached then security violation modes lead to protect, restrict or shutdown of port.

There are 3 ways how to configure port security:

1) Static secure MAC addresses – manually configured with

   switchport port-security mac-address MAC_ADDRESS

2) Dynamic secure MAC address – dynamic learned and stored only in address table (after restart cleared)

3) Sticky secure MAC address – *mac address are learned dynamically and saved in running config (next can be merged with startup config)*.

Default port security:

– *disabled on port* -> switchport port-security

– *maximum nr. of secure MAC*: 1

– *violation mode*: shutdown

– *sticky address learning*: disabled

Sample configs:

A) **Dynamic port security configuration**

```
s1#configure terminal

s1(C)# interface FastEthernet0 0/10
```

```
s1(c-if)#switchport mode access

s1(c-if)#switchport port-security

s1(c-if)#end
```

B) **Sticky port security** – can configure max. nr. of secure mac address, in this example we configure shutdown as the violation mode

```
s1#configure terminal

s1(C)# interface FastEthernet0 0/10

s1(c-if)#switchport mode access

s1(c-if)#switchport port-security     (enable port security)

s1(c-if)#switchport port-security maximum 20 (maximum nr. of secure address)

s1(c-if)#switchport  port-security  mac-address  sticky
 (enable sticky learning)

s1(c-if)#end
```

Table: *Security violation modes*

Violation mode	Forward traffic	Send syslog message	Display error message	Increase violation counter	Shuts down port
protect	no	no	no	no	no
restrict	no	yes	no	yes	no
shutdown	no	yes	no	yes	yes

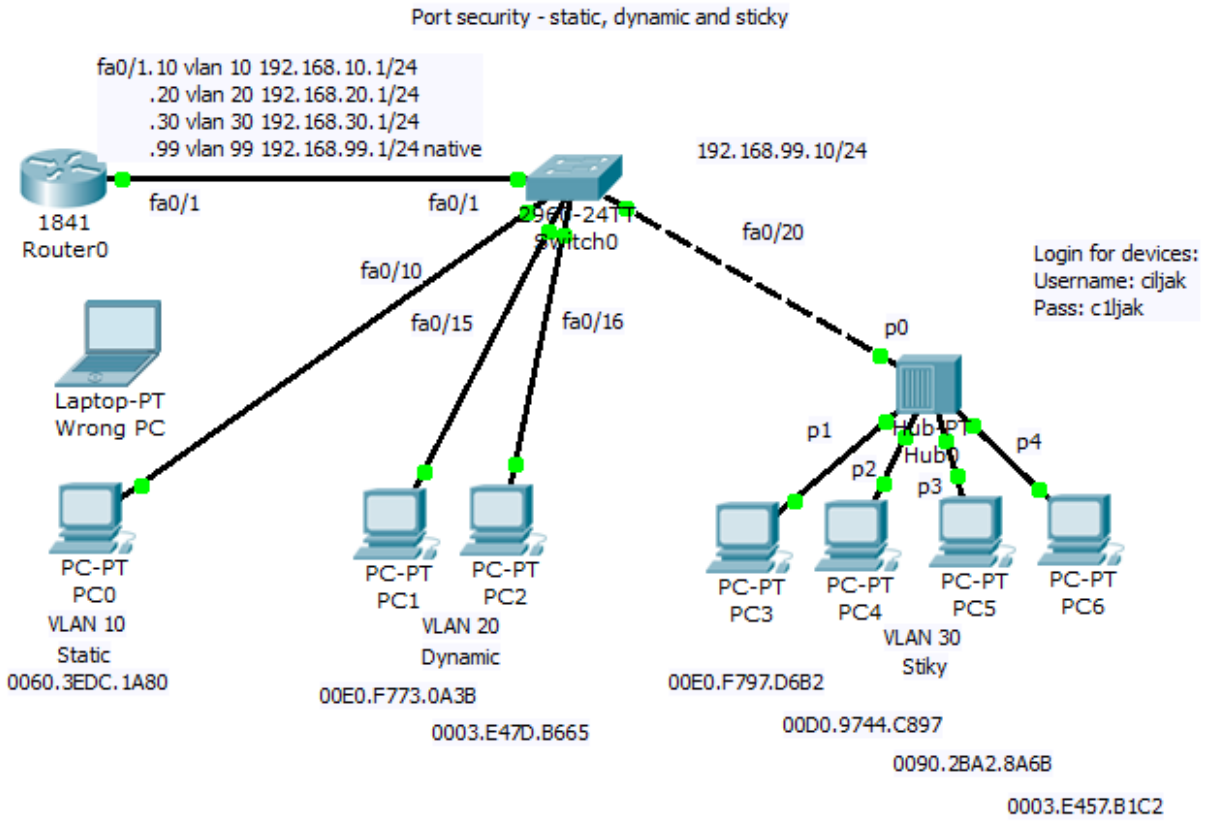
Verification commands:

- show port-security [interface interface-id]

```
Switch#show port-security interface fa0/10
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Shutdown
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   : 0000.0000.0000:0
Security Violation Count   : 0
```

- show port-security [interface interface-id] address

Our training scenario focused on port-security can be obtained from here (Packet tracer 5.2 or above you will need).



Network topology consist of router acting on stick and switch. Port security is configured sticky for 10 mac address for port 20 to 24 with commands:

```
interface FastEthernet0/20
 switchport access vlan 30
 switchport port-security maximum 10
 switchport port-security mac-address sticky
!
```

```
interface FastEthernet0/21
 switchport access vlan 30
 switchport port-security maximum 10
 switchport port-security mac-address sticky
!
interface FastEthernet0/22
 switchport access vlan 30
 switchport port-security maximum 10
 switchport port-security mac-address sticky
!
interface FastEthernet0/23
 switchport access vlan 30
 switchport port-security maximum 10
 switchport port-security mac-address sticky
!
interface FastEthernet0/24
 switchport access vlan 30
 switchport port-security maximum 10
 switchport port-security mac-address sticky
```

You are strongly encouraged to try

1) *Static port security for PC on vlan 10 on port fa0/10 with mac 0060.3EDC.1A80* – then disconnect device with mentioned mac and attach device with wrong mac (examine shuting down state of port), then correct port state and enable traffic forwarding.

```
interface FastEthernet0/10
 switchport access vlan 10
 switchport port-security mac-address 0060.3EDC.1A80
!
```

2) *Enable dynamic learning for PC on ports fa0/15 and fa0/16.*

As example, output from show mac-address-table of switch

```
Switch#sh mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  10    0060.2fcc.9102    DYNAMIC     Fa0/1
  10    0060.3edc.1a80    DYNAMIC     Fa0/10
  20    0003.e47d.b665    DYNAMIC     Fa0/16
  20    0060.2fcc.9102    DYNAMIC     Fa0/1
  20    00e0.f773.0a3b    DYNAMIC     Fa0/15
  30    0003.e457.b1c2    DYNAMIC     Fa0/20
  30    0060.2fcc.9102    DYNAMIC     Fa0/1
  30    0090.2ba2.8a6b    DYNAMIC     Fa0/20
  30    00d0.9744.c897    DYNAMIC     Fa0/20
  30    00e0.f797.d6b2    DYNAMIC     Fa0/20
  99    0060.2fcc.9102    DYNAMIC     Fa0/1
Switch#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,30,99
```

On port fa0/20 can be spot shared network segment (in our case it is hub interconnected segment).