PORTBIZTONSÁG ÉS VLAN-OK

Portbiztonság:

- alkalmazásakor célunk a hálózati biztonság kialakítása, a hálózat biztonságosabbá tétele
- egyes eszközök interfészein konfigurálhatjuk a szabályainkat
- Lehetőségeink:
  - megadhatjuk az egy porthoz maximálisan csatlakoztatható MAC-címek számát
  - megadhatjuk az adott portra csatlakoztatandó eszközök konkrét MAC-címeit.
  - megadhatjuk, hogy mi történjen, amennyiben megsértik a portbiztonsági szabályunkat:
    - „protect” állapot: csak eldobja a switch a keretet
    - „restrict” állapot: eldobja a keretet a switch, és naplózza is a sértő eszköz MAC-címét, illetve a behatolási kísérletek számát
    - „shutdown” állapot: ugyanaz gyakorlatilag, mint a restrict állapot, csupán annyival tud többet, hogy a portbiztonság megsértése esetén a portot „disabled” állapotba helyezi → ezt csak manuálisan, kézi beavatkozással (a port ki-be kapcsolásával) állítható vissza

Portbiztonság konfigurálása:

```
Switch (config) #int fa0/1
Switch (config-if) #switchport mode access
Switch (config-if) #switchport port-security mac-address sticky
```

vagy általunk megadott címmel:

```
Switch (config-if) #switchport port-security mac-address 0123.4567.89AB
Switch (config-if) #switchport port-security violation shutdown
```

ha nem szeretnénk, hogy letiltson:

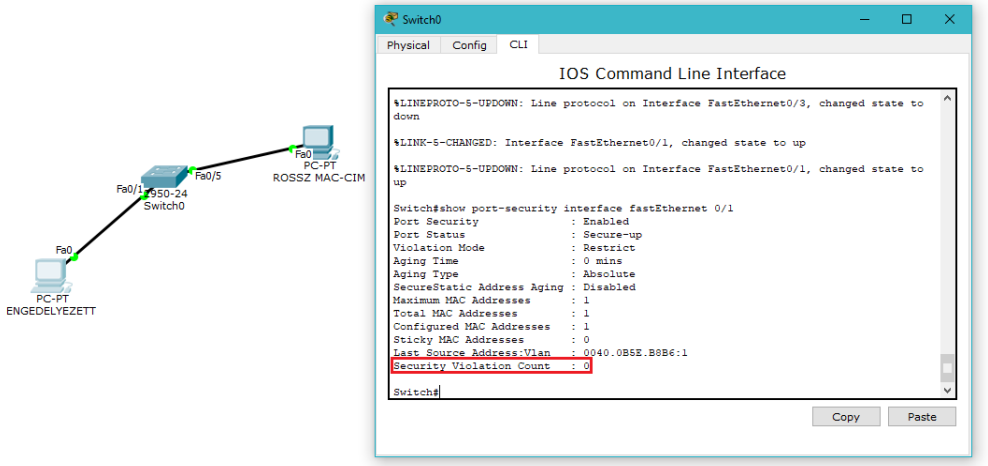
```
Switch (config-if) #switchport port-security violation [ protect
                   | restrict ]
```

Portbiztonság miatt letiltott port újraengedélyezése:

```
Switch (config) #int fa0/1
Switch (config-if) #shutdown
Switch (config-if) #no shut
```

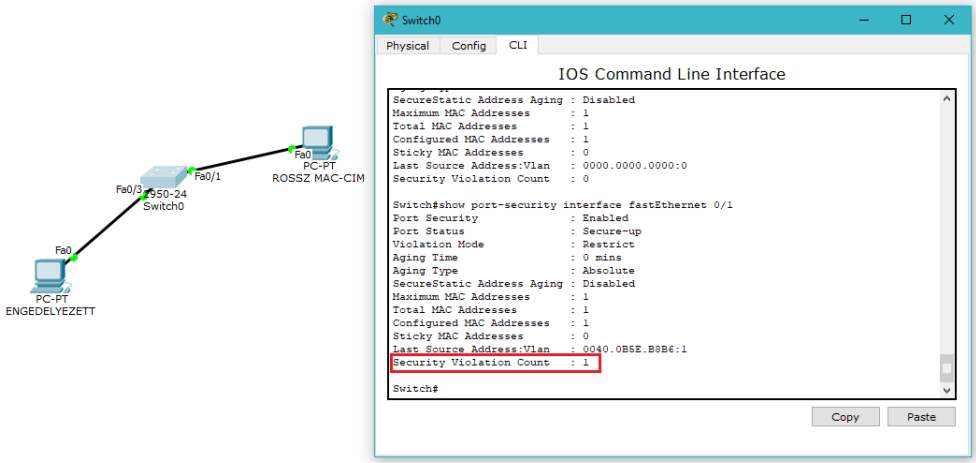
Példák:

A switch FastEthernet 0/1 portján bekonfiguráltam egy portbiztonsági beállítást a fönti parancsok segítségével, melyben megadtam az „ENGEDELYEZETT” PC MAC-címét, így kijelölve, hogy ezen az interfészen csak ezt az egy gépet kívánom engedélyezni.



Ezután, az eszköz csatlakoztatása után a `Switch#show port-security interface fastEthernet 0/1` parancs segítségével lekértem az interfész portbiztonsági adatait, és azt tapasztaltam, hogy a jól működő, élesített szabályom nem észlelt illetéktelen behatolási kísérletet (lásd: piros téglalappal jelölt terület).

Azonban, mikor újrakonfiguráltam a hálózatot, és ezúttal az ismeretlen MAC-címmel rendelkező gépet csatlakoztattam a FastEthernet 0/1 számú porthoz, már láthatjuk: merőben más a helyzet.



VLAN:

← problémát jelentett, hogy a kapcsolókból álló hálózaton mindenki képes volt mindenkivel kommunikálni, akkor is, ha ez szükségtelen volt

- feleslegesen nagy szórási tartományok, ütközések valószínűsége, forgalom nagysága
- skálázhatóság, hálózati menedzsment, biztonság igénye

A probléma megoldására jönnek létre a **vlanok**

- céljuk, hogy szegmentálják a hálózatot, leredukálják a felesleges szórások számát
- olyan működési mechanizmust tesznek elérhetővé switcheken, melyeket a routerek biztosítanak(ezek a 3. rétegbeli IP-alhálózatok, vagyis subnetek) lanok esetén (bár a két konstrukció más-más réteghez tartozik, mégis fontos tényező a hálózattervezésnél a kapcsolatuk, és a gyakorlatban általában egy-az-egyben megfeleltetik őket egymásnak)
- előnyei: hálózati terhelés kontrollálhatósága, biztonságosabb, virtuális munkacsoportok rugalmas, dinamikusabb hálózatkarbantartást tesz lehetővé azáltal, hogy gyorsan reagálhatunk a gépek áthelyezésére → egyszerűbb adminisztráció
- az azonos vlanhoz rendelt hostokat nem határolja be a fizikai topológia és a távolság, csak virtuális határok vannak
- különböző vlanok nem látják egymás forgalmát
- az IEEE 802.1Q szabvány használata: ennek használatával megjelenik egy új mező az Ethernet fejlécében, így a vlan már nem csak lokálisan (switchen belül) értelmezhető, hanem nagyobb hálózatra is kiterjed

Port fajták:

- Acces port: klienseknél, ún. buta eszközöknél használjuk, nem tagelt mód, csak egy VLAN forgalmát kezeli, és továbbítja
- Trunk port: több VLAN forgalmát kezeli, tagelt mód

VLAN fajtái:

- alapértelmezett – alapvetően minden port itt van, CISCO eszközök esetén ez a vlan a VLAN 1, nem átnevezhető, de minden funkcióval bír
- adat – „felhasználói VLAN”, a felhasználó generálta adatforgalom átvitelére használatos, azért használjuk, hogy el tudjuk különíteni a többi fajta VLAN adatforgalmától a felhasználóit, és így nagyobb kontrollal bírjunk a hálózat fölött
- natív – a 802.1Q szabvány találmánya, amikor tageletlen (címke nélküli, nem VLAN-ból érkező) csomag érkezik, a trunk port a csomagot a natív VLAN-ba helyezi → így tudunk nem tagelt csomaggal is dolgozni, kompatibilitás
- menedzsment – lehetővé teszi, hogy távoli eszközökről konfiguráljuk a switch-ünket, általában itt használunk FTP, SSH protokollt, szenzitív adatot forgalmaz, így nem érdemes a VLAN 1-re állítani
- voice – VOIP, hangátvitelnél használatos, prioritást élvez sávszélesség tekintetében a hálózaton a megfelelő kapcsolat érdekében

Konfigurálása:

VLAN-ok létrehozása:

Első módszer:

```
Switch#vlan database
Switch(vlan)#vlan 10 name alfa
VLAN 10 added:
   Name: alfa
Switch(vlan)#vlan 100 name beta
VLAN 100 added:
   Name: beta
```

Második módszer:

```
Switch(config)#vlan 25
Switch(config-vlan)#name gamma
```

Portok hozzárendelése adott VLAN-hoz:

```
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
```

Egyszerre több port hozzárendelése:

```
Switch(config)#int range fa0/10 - 15
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 25
```

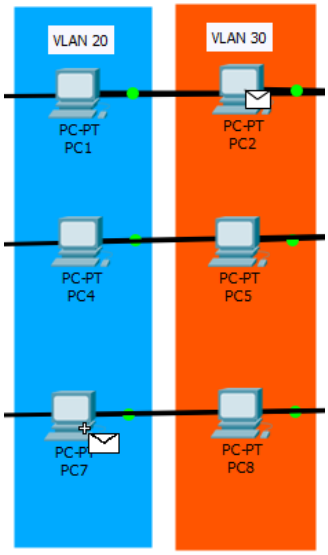
Trönkport beállítása:

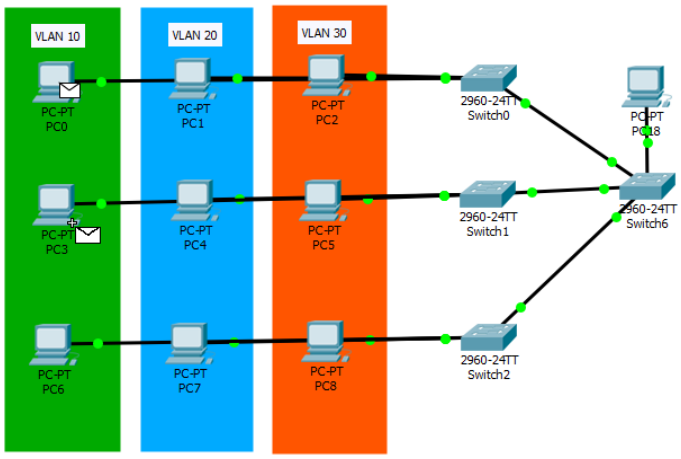
```
Switch(config)#int fa0/24
Switch(config-if)#switchport mode trunk
```

Natív VLAN beállítása (a trönk mindkét végén meg kell adni!):

```
Switch(config-if)#switchport trunk native vlan 99
```

Példa: a VLAN 10-es gépek képesek egymással kommunikálni, míg a VLAN 30 képtelen elérni a VLAN 20-at.





Last Status	Source	Destination
Successful	PC0	PC3
Failed	PC2	PC7