Kapcsolók portbiztonsága

1. Elmélet:
   - A kapcsolók az ISO OSI referencia modell 2. rétegében működnek.
   - A 2. rétegben is számtalan támadás érheti a hálózatokat.
   - A kapcsolókban számos biztonsági lehetőség létezik, ezeket megfelelőenkell konfigurálni.
   - A forgalomirányítókhoz hasonlóan a kapcsolókban is rendelkezésre állnak a hozzáférési listák (ACL) a magasabb rétegben működő protokollokvédelmére.
     alkalmazásakor célunk a hálózati biztonság kialakítása, a hálózat biztonságosabbá tétele
   - egyes eszközök interfészein konfigurálhatjuk a szabályainkat
2. 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

3. Switchek portbiztonsága:

Beállítás lépései:

- A kapcsoló portjának beállítása hozzáférési módba
- Portbiztonság engedélyezése
- Maximális eszköz számának megadása
- Hogyan „tanulja meg” az engedélyezett fizikai címeket
- Büntetés típusának megadása

Parancsok:

S_Server(config)#**interface** *F0/1*

S_Server(config-if)#**switchport mode access**

S_Server(config-if)#**switchport port-security**

S_Server(config-if)#**switchport port-security maximum 1**

S_Server(config-if)#**switchport port-security mac-address sticky**

S_Server(config-if)#**switchport port-security violation shutdown**

Magyarázat:

A „switchport mode access” hozzáférhetővé teszi a portot kézi beállítások számára. Ha ezt nem állítjuk be, a port dinamikus módban van, és nem állítható be hozzá a portbiztonság.

A „switchport port-security” parancs kiadásával a portot portbiztonság üzemmódba kapcsoljuk. Ez mindenképpen önállóan is ki kell adni. Ezek után ugyanezen parancs alparancsaival manipuláljuk tovább a portot.

Az első alparancs beállítja a csatlakozó eszközök maximális számát. A példában ez egy.

A második mac-address sticky, azt jelenti az elsőként csatlakozó gép IP címét engedélyezett. A switch ezt a MAC címet megjegyzi. Ezt nevezzük tanuló módnak. De kézzel is beállíthatunk egy MAC címet, ponttal tagolva, ahogy Cisco eszközökben ezt megszoktuk. (Pl.: **switchport port-security mac-address 00E0.8F69.69BA**)

Az utolsó a büntetés típusát adja meg.

```
S1(config-if)#switchport port-security violation [ protect | restrict | shutdown ]
```

Büntetési módok					
Büntetés módja	**Forgalom továbbítása**	**Syslog üzenet küldése**	**Hibaüzenetek mutatása**	**Növeli a büntetés számlálót**	**Port leállítása**
protect	nem	nem	nem	nem	nem
restrict	nem	igen	nem	igen	nem
shutdown	nem	igen	nem	igen	igen

Kikapcsolás:

```
enable
configure terminal
int f0/1
no switchport mode access
no switchport port-security
no switchport port-security mac-address sticky
```

```
enable
clear port-security all
conf t
int f0/1
shutdown
no shutdown
```