Kapcsolóbeállítások

Lokális felhasználó létrehozása nem titkosított és titkosított jelszóval:

Switch(config)#username admin password cisco

Switch(config)#username boss secret class

Felügyeleti interfész beállítása

A kapcsolók alapértelmezetten nem rendelkeznek IP címmel. A sávos eléréshez, azonban szükség van rá, de a portokhoz nem rendelhetők IP címek. Ezért virtuális interfészhez rendeljük az IP címet.

```
S1(config)#interface vlan 99
S1(config-if)#ip address 192.17.25.4 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#end
```

Port duplex módja és sebessége

```
S1(config)# interface FastEthernet 0/1
S1(config-if)# duplex full
S1(config-if)# speed 100
S1(config-if)# end
```

auto-MDIX

Az auto-MDIX bekapcsolása lehetővé teszi, hogy egy interfészre csatlakoztatott kábelt a kapcsoló automatikusan felismerjen és a kábel típusának megfelelően konfiguráljon. Így használható **egyenes és keresztkötésű kábel** is.

Az mdix beállítása:

```
S1(config-if)# mdix auto
```

Teljes lista:

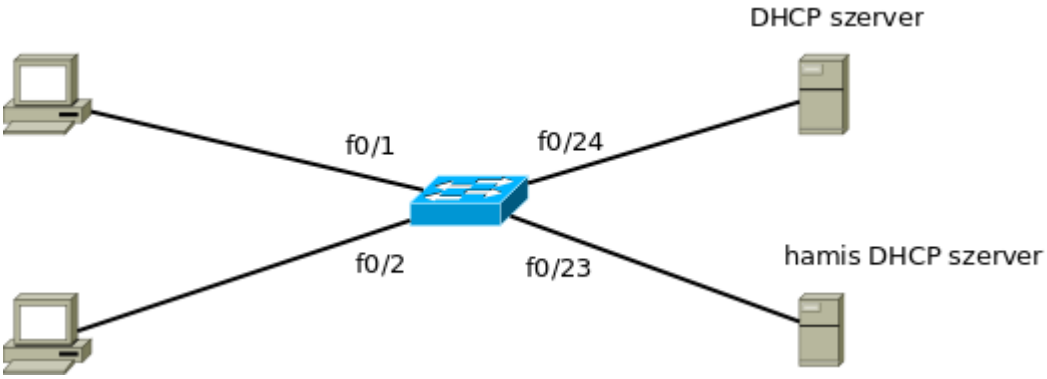
```
S1(config)# interface fastethernet 0/1
S1(config-if)# duplex auto
S1(config-if)# speed auto
S1(config-if)# mdix auto
S1(config-if)# end
```

Ellenőrzés:

```
S1# show controllers ethernet-controller fa 0/1 phy | include Auto-MDIX
```

DHCP-snooping

Beállíthatjuk a kapcsoló melyik portján érkezhetnek DHCP válaszok. A többi porton tiltott.



A legegyszerűbb lehetőség, amikor kijelöljük melyik port megbízható. Ehhez, az interfészen az ip dhcp snooping trust parancsot használjuk:

```
S2(config)# ip dhcp snooping
S2(config)# interface fastethernet 0/24
S2(config-if)# ip dhcp snooping trust
```

Tekintsük meg az eredményt:

```
S1#show ip dhcp snooping
```

Lehetséges kimenet:

```
S1#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
none
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/1            no         unlimited
FastEthernet0/23           no         unlimited
FastEthernet0/24           yes        unlimited
```

Ha van VLAN, beállíthatjuk melyiket szeretnénk védeni.

```
S2(config)# ip dhcp snooping vlan 10,20
```

Azokon a portokon, ahol DHCP kliensek várható, beállíthatjuk hogy ne legyen túl sok kérés másodpercenként. Például 5 másodpercenként fogadunk el kéréseket:

```
S2(config-if)# interface range fa0/2 - 10
S2(config-if-range)# ip dhcp snooping limit rate 5
```

Egy teljes lista:

```
S2(config)# ip dhcp snooping
S2(config)# ip dhcp snooping vlan 10,20
S2(config)# interface fastethernet 0/1
S2(config-if)# ip dhcp snooping trust
S2(config-if)# interface range fa0/2 - 10
S2(config-if-range)# ip dhcp snooping limit rate 5
```

- A DHCP snooping engedélyezése: ip dhcp snooping.
- A DHCP snooping engedélyezése a 10 és 20-as VLAN-on: ip dhcp snooping vlan 10,20.
- Adott port beállítása biztonságosra: ip dhcp snooping trust.

- Hamis DHCP kérések számának korlátozása: ip dhcp snooping limit rate kérések_száma.

Portbiztonság beállítása

A portok alapértelmezetten nyitottak, védelem nélkül. A biztonság érdekében érdemes néhány biztonsági beállítást megadni. Az úgynevezett portbiztonság a switchport parancson alapszik, amit egy interfészen kell beállítani.

```
S1>en
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int f0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#
S1(config-if)#switchport port-security maximum 2
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#switchport port-security violation shutdown
```

Vegyük szemügyre az egyes beállításokat. 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 alparancsok sorba:

1. switchport port-security maximum 2
2. switchport port-security mac-address sticky
3. switchport port-security mac-address aaaa.aaaa.aaab
4. switchport port-security violation shutdown

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

A második *mac-address sticky*, azt jelenti az elsőként csatlakozó gép MAC 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.

Az utolsó a büntetés típusát adja meg.

Büntetési beállítások:

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

Büntetés címén háromféle beállítás adható meg. Ezek a *protect, restrict* és a *shutdown*. Alapértelmezés a *shutdown*. A következő táblázat bemutatja, az egyes beállításoknak milyen következményei lesznek.

	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

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

Ellenőrzések:

```
S1#show port-security interface fastethernet 0/18
S1#show run
S1#show port-security address
S1#show mac-address-table
```

Egy port ellenőrzése:

```
S1#sh port-security int f0/1
```

Lehetséges kimenete:

```
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Ez a bejegyzés: „Sticky MAC Addresses : 0”, a megtanult MAC címet mutatja. A „Last Source Address:Vlan : 0000.0000.0000:0” bejegyzés mutatja, melyik eszközről látogatták a portot utoljára. A „Security Violation Count” a kiszabott büntetések száma.

Kikapcsolás f0/1 porton:

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

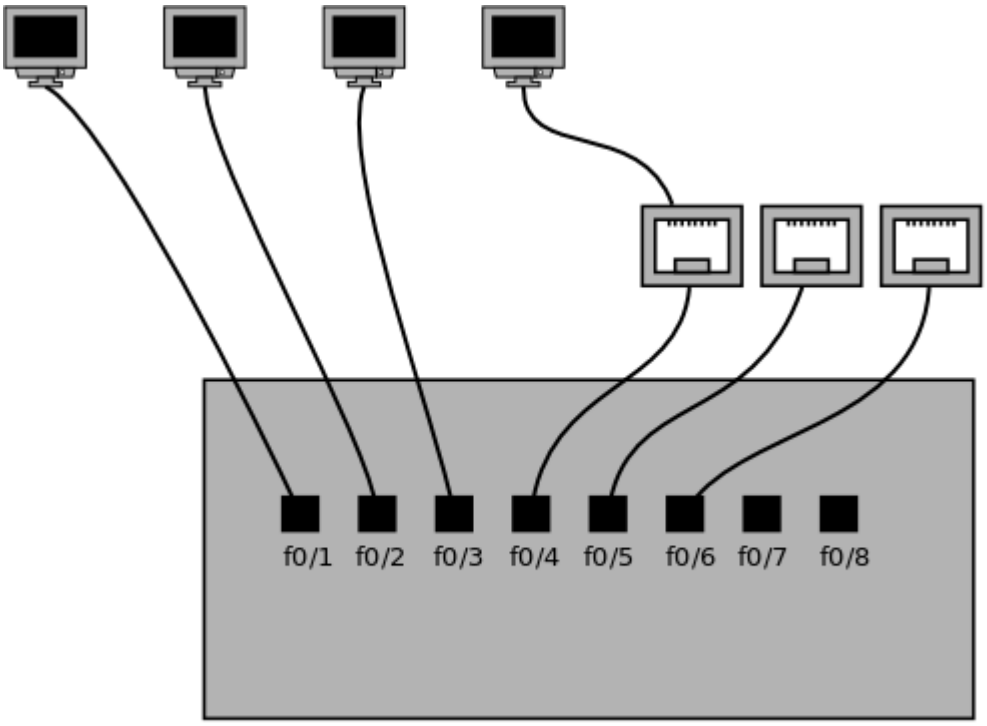
Külön ki kell kapcsolni a mac-address-t.

Port visszakapcsolása Secure-shutdown után:

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

Nem használt portok leállítása

A nem használt portok, amennyiben nincsenek letiltva, és egy fali dugaszolóaljzatban végződnek, egy illetéktelen személy hozzáférhet a belső hálózatunkhoz.



Erre megoldás az ilyen portok leállítása:

Egy nem használt port tiltása:

```
S1(config)#int f0/8
S1(config-if)#shutdown
```

A példában a f0/8-s portot tiltottuk le.

Több nem használt port tiltása, tartomány megadásával:

```
S1(config)#interface range f0/5-7
S1(config-if)#shutdown
```

A példában a 5-7-ig az összes portot letiltottuk.

CDP

A **CDP** a **Cisco Discovery Protocol** rövidítése. A Cisco eszközök arra használják, hogy felderítsék a szomszédos Cisco eszközöket. Információt cserélnek arról, melyik port milyen másik eszközhöz csatlakozik. Megmondják egymásnak milyen IP címen vannak beállítva, milyen képességei vannak az eszköznek.

Ismeretlen eszközök felé kockázatos ilyen információt küldeni, vagy onnan fogadni. Az egyes eszközökön a CDP protokoll használata így ki vagy bekapcsolható. A nem ismert eszközök hamis információkat terjeszthetnek magukról.

Ha egy támadó egy Cisco eszközről kideríti milyen típusú, mik vannak rajta beállítva, milyen verzió, a hibalista birtokában könnyen támadást intézhet. Egy támadó Cisco telefonnak állíthatja be magát, így hozzáférve a Voice VLAN-hoz.

Mit tegyünk?

- csak akkor kapcsoljuk be, ha szükségünk van CDP információkra
- használat után kapcsoljuk ki
- külvilág fel tiltsuk le
- csak adott portra kapcsoljuk be

A CDP alapértelmezetten be van kapcsolva. A következőképpen kapcsolhatjuk ki globálisan:

```
S1(config)# no cdp run
```

Visszakapcsolás globálisan:

```
S1(config)# cdp run
```

Bekapcsolhatjuk csak adott porta:

```
S1(config-if)# cdp enable
```

Ezek a beállítások természetesen útválasztón is használhatók.